S. Hrg. 99-166

FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

HEARINGS

BEFORE THE

PERMANENT
SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

NINETY-NINTH CONGRESS

FIRST SESSION

APRIL 16, 17, 18, AND 25, 1985

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
49-958 O WASHINGTON : 1985

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, DC 20402

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, Jr., Delaware, *Chairman*

TED STEVENS, Alaska
CHARLES McC. MATHIAS, Jr., Maryland
WILLIAM S. COHEN, Maine
DAVID DURENBERGER, Minnesota
WARREN B. RUDMAN, New Hampshire
THAD COCHRAN, Mississippi

THOMAS F. EAGLETON, Missouri
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio
CARL LEVIN, Michigan
ALBERT GORE, Jr., Tennessee

John M. Duncan, *Staff Director*
Margaret P. Crenshaw, *Minority Staff Director*

Permanent Subcommittee on Investigations

WILLIAM V. ROTH, Jr., Delaware, *Chairman*
WARREN B. RUDMAN, New Hampshire, *Vice Chairman*

CHARLES McC. MATHIAS, Jr., Maryland
WILLIAM S. COHEN, Maine
THAD COCHRAN, Mississippi
TED STEVENS, Alaska

SAM NUNN, Georgia
LAWTON CHILES, Florida
JOHN GLENN, Ohio
CARL LEVIN, Michigan
ALBERT GORE, Jr., Tennessee

Daniel F. Rinzel, *Chief Counsel*
Eleanore J. Hill, *Chief Counsel to the Minority*
Katherine Bidden, *Chief Clerk*

CONTENTS

Opening statements: Page
- Senator Nunn 1
  - Senator Nunn's closing statement 781
- Senator Gore 6
- Senator Roth 19
- Senator Chiles 22
- Senator Cohen 413

WITNESSES

Tuesday, April 16, 1985

Bill W. Thurman, Deputy Director, National Security and International Affairs Division, General Accounting Office, accompanied by Irving Boker, Assignment Manager, and James Reid, GAO Evaluator 7

Brig. Gen. Charles F. Scanlon, Deputy Commander, Intelligence Command, Department of the Army 61

Sergeant "Smith," U.S. Army 93

Fred Asselin, staff investigator for the minority, Permanent Subcommittee on Investigations 104

Phillip A. Parker, Deputy Assistant Director, Intelligence Division, Federal Bureau of Investigation, accompanied by Joseph D. Domzalski, Assistant Section Chief, Civil Rights and Special Inquiry Section, and Harry W. Porter III, Unit Chief, Intelligence Division, Non-Soviet Research and Analysis 151

Wednesday, April 17, 1985

Donald J. Devine, Office of Personnel Management 195

A. Barry Dalinsky, Deputy Director of Security Division, Department of Energy 314

Lawrence J. Howe, vice president, corporate security, Science Applications International Corp., La Jolla, CA; and Eli S. Flyer, consultant, Manpower Research Center, Department of Administrative Sciences, Naval Postgraduate School, Monterey, CA 356

Thursday, April 18, 1985

Thomas J. O'Brien, Director, Defense Investigative Service, Department of Defense 416

Christopher J. Boyce 493

Gen. John W. Pauly, USAF (retired), Systems Control Technology, Inc., Palo Alto, CA; Paul W. Schwegler, vice president and general manager, administrative services division, TRW, Inc., electronics and defense sector, Redondo Beach, CA; and Richard M. Welby, assistant director of corporate security, Hughes Aircraft Co., El Segundo, CA 513

Thursday, April 25, 1985

Gen. Richard G. Stilwell, USA (retired), Deputy Under Secretary of Defense for Policy, accompanied by L. Britt Snider, Director, Counterintelligence and Security Policy, Department of Defense; William R. Fedor, Deputy Director Counterintelligence and Investigative Programs; and Kathleen A. Buck, Assistant General Counsel, Department of Defense 618

Alphabetical List of Witnesses

Page
Asselin, Fred:
  Testimony 104
  Chronology of events concerning Veliotis 111
Boker, Irving: Testimony 7
Boyce, Christopher J.: Testimony 493
Buck, Kathleen A.:
  Testimony 618
  Prepared statement with attachments 706
  Responses to written questions 776
Dalinsky, A. Barry:
  Testimony 314
  Prepared statement 323
  Responses to written questions 344
Devine, Donald J.:
  Testimony 195
  Prepared statement with attachments 222
  Responses to written questions 287
Domzalski, Joseph D.: Testimony 151
Fedor, William R.: Testimony 618
Flyer, Eli S.:
  Testimony 356
  Prepared statement with attachments 400
Howe, Lawrence J.:
  Testimony 356
  Prepared statement with an attachment 371
  Responses to written questions 389
O'Brien, Thomas J.:
  Testimony 416
  Draft legislation 421
  DISP facilities rated unsatisfactory in fiscal year 1984 433
  Prepared statement with attachments 441
  Responses to written questions 489
Parker, Phillip A.:
  Testimony 151
  Prepared statement with attachment 160
  Responses to written questions 188
Pauly, Gen. John W.:
  Testimony 513
  Prepared statement 539
  Responses to written questions 545
Porter, Harry W., III: Testimony 151
Reid, James: Testimony 7
Scanlon, Brig. Gen. Charles F.:
  Testimony 61
  Prepared statement with attachments 65
  Responses to written questions 89
Schwegler, Paul W.:
  Testimony 513
  Prepared statement 550
  Responses to written questions 562
"Smith," Sergeant: Testimony 93
Snider, L. Britt: Testimony 618
Stilwell, Gen. Richard G.:
  Testimony 618
  Prepared statement 642
  Responses to written questions 659
Thurman, Bill W.:
  Testimony 7
  Prepared statement with attachments 26
  Responses to written questions 59
Welby, Richard W.:
  Testimony 513
  Prepared statement with attachments 575
  Responses to written questions 611

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Page
Personnel Security Program, submitted by A. Barry Dalinsky, Deputy Director of Security Division, Department of Energy ... 783
Comparison: Background investigations by OPM and DIS, submitted by the Permanent Subcommittee on Investigations ... 874

Statements of:

- Aerojet General, Jeremiah M. Dolan, corporate director of security and administrative services, Aerojet General, and industry adviser, Industrial Review Committee ... 875
- Central Intelligence Agency ... 880
- Department of the Air Force, Directorate of Information Security, Air Force Office of Security Police ... 894
- Department of the Army, Col. Charles J. Little, Chief, Office of Security, Defense Intelligence Agency [DIA] ... 908
- Department of the Army, Office of the Assistant Chief of Staff for Intelligence ... 935
- Department of the Navy, Rear Adm. John L. Butts, Director of Naval Intelligence ... 955
- Department of State ... 964
- DOD Industrial Security Review Committee, Daniel R. Foley and John R. Hancock, co-chairmen ... 973
- General Services Administration, Steven Garfinkel, Director, Information Security Oversight Office [ISOO] ... 985
  - Information Security Oversight Office's [ISOO] 1984 report to the President ... 1000
  - President Reagan's response to the report, April 29, 1985 ... 1038
- Larson, Dr. Robert E ... 1039
- Lockheed Missiles & Space Co., Inc ... 1048
- National Security Agency, Philip T. Pease, Director of Security ... 1073
- Nuclear Regulatory Commission ... 1086
- 3-M, P.J. Muldowney, marketing director, Safety & Security Systems Division and J.E. Klinzing, government markets manager, Office of Systems Division ... 1101

EXHIBITS

	Introduced on page	Appears on page
1. "Analysis of the Effectiveness of the Department of Defense Industrial Security Program and Recommendations for Program Improvement," a report to the Deputy Under Secretary of Defense Industrial Security Review Committee, December 10, 1984	1	1113
2. Executive Order 10450	5	*
3. "The Impact of Case Law and Privacy on the Federal Employee Loyalty-Security Program," Richard Ehlke, Congressional Research Service, Library of Congress, November 2, 1984	5	1177
4. "Personnel Security Investigations for National Security and Intelligence Employees," Frederick M. Kaiser, Congressional Research Service, Library of Congress, February 8, 1985	5	1187
5. Descriptions of personnel security policies and procedures of several NATO allies and France, prepared by Dr. Edith Palmer, et al., Congressional Research Service, Library of Congress, June 10, 1985	5	1211
6. "Personnel Security Investigations and National Security: Selected References," bibliography, Sherry B. Shapiro, Congressional Research Service, Library of Congress, June 4, 1985	5	1261
7. Memorandum for Robert C. McFarlane, Assistant to the President for National Security Affairs from Mary C. Lawton, Department of Justice regarding NSDD-84 Study of Federal Personnel Security Program, May 1, 1984	5	1274
8. Memorandum from William French Smith, Attorney General, on Presidential Directive on Safeguarding National Security Information, March 11, 1983	5	1282

EXHIBITS—Continued

	Introduced on page	Appears on page
9. Letter, with enclosure, to Senator Nunn from Paul E. Trayers, legislative counsel, U.S. Merit Systems Protection Board, regarding *Hoska* v. *Department of the Army*, 677 F. 2d 131 (D.C. Cir. 1982), February 20, 1985	5	1302
10. Charts by the Department of Defense: "Cleared Soviet Emigres," "Emigres from Foreign Countries," and "DISCO: Number of Contractors Submitting 6.b.1 Reports"	5	1307
11. Statement and attachments from Jack Brooks, chairman, House Committee on Governmental Operations, April 29, 1985	5	1310
12. Chronology of pertinent events concerning Veliotis	105	111
13. Summary statement by the Energy Department apparently used by the Department in adjudicating Veliotis' 1977 application for a "Q" access authorization	105	149
14. Documents from which Mr. Asselin's summary chronology was drawn	105	*
15. Letter to Caspar W. Weinberger, Secretary of Defense, from Donald J. Devine, Director, Office of Personnel Management, January 16, 1985	206	207
16. Letter to Donald J. Devine, Director, Office of Personnel Management, from Caspar W. Weinberger, Secretary of Defense, February 7, 1985	206	210
17. Basic Installment 311 and critical reports pertaining to it	212	*
18. "Government is Drafting Electronic Security Rules," article by Michael Strange, Washington Post, April 18, 1985	414	414
19-25. Photographs of the "black vault" at TRW, Inc	509	1335
26. Volumes pertaining to Hughes Aircraft Co. Security Program, 1985	525	*

---

*May be found in the files of the subcommittee.

FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

TUESDAY, APRIL 16, 1985

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The subcommittee met, at 9:38 a.m., in room SD-342, Dirksen Senate Office Building, under authority of Senate Resolution 85, section 13, dated February 28, 1985, Hon. William V. Roth, Jr. (chairman), presiding.

Members of the subcommittee present: Senator William V. Roth, Jr., Republican, Delaware; Senator William S. Cohen, Republican, Maine; Senator Sam Nunn, Democrat, Georgia; Senator Lawton Chiles, Democrat, Florida; and Senator Albert Gore, Democrat, Tennessee.

Members of the professional staff present: Daniel F. Rinzel, chief counsel; Eleanore J. Hill, chief counsel to the minority; Katherine C. Bidden, chief clerk; John F. Sopko, assistant counsel to the minority; David Glendinning, staff counsel; Leonard A. Willis, Glenn W. Fry, and Fred Asselin, investigators for the minority; Sarah Presgrave, executive assistant to the chief counsel; Kathleen A. Dias, executive secretary to the chief counsel to the minority; and Mary Robertson, assistant chief clerk to the minority.

[Senators present at the convening of the hearing: Senators Nunn and Gore.]

OPENING STATEMENT OF SENATOR NUNN

Senator NUNN. The subcommittee will come to order.

Chairman Roth has been delayed inadvertently here and has asked me to go ahead and begin the hearings. I will do so. When he comes, he will be making an opening statement. In the meantime, I will proceed with mine in order to keep the hearings on time as much as possible because we do have a rather long agenda today.

The Senate Permanent Subcommittee on Investigations today begins 3 days of public hearings on the effectiveness of the Government's personnel security programs.

The hearings, which are based on an investigation by the subcommittee minority staff, will enable members to evaluate the efforts by several agencies of the executive branch to establish the integrity and reliability of persons applying for and working in Federal positions and contractor employment.

At the outset, I want to thank Chairman Roth for the fine cooperation that our minority staff has received throughout the course of this investigation. The majority staff has been most cooperative, and we appreciate their support and assistance in making these hearings possible.

This subcommittee's interest in personnel security stems in part from our past concern over the transfer of American high technology to the Soviet Union and Soviet bloc nations. In examining that issue, we found that individuals holding high Government security clearances had sold some of this country's most guarded high technology secrets to hostile intelligence services.

As one example, William Holden Bell, a former Hughes Aircraft engineer, now convicted of espionage, who testified before this subcommittee, told the subcommittee that despite obvious financial and personal problems and a security clearance he believed was 28 years old, his access to highly sensitive documents was never questioned.

When you think about a security clearance being 28 years old, it seems incredible. Yet, if you look at the numbers which I will relate in a moment, it becomes much more understandable.

Cases such as the Bell case suggested critical shortcomings in the Government Personnel Security Program, and it prompted our investigation which led to these hearings. I expect that much of the testimony we will hear over the next few days will confirm that there is ample room for improvement in the way our Government ensures the integrity of those persons who have access to highly classified secrets.

Today, the Government's Personnel Security Program for Federal employees still operates under the provisions of an Executive order issued more than 32 years ago, despite numerous recommendations over the years that it be revised and substantially updated.

The Government's personnel security program for contractor personnel is only slightly more current, operating under an Executive order some 24 years old. By contrast, the FBI tells us today that Soviet spies in the United States are "more numerous, sophisticated, and aggressive than ever before." Today the U.S. Department of Justice reports the highest number of pending espionage cases since World War II.

Evidently, hostile intelligence services are not overly intimidated by our Government's Personnel Security Program. This morning, we will hear testimony from a U.S. Army sergeant who for more than 10 years dealt with the Soviets as a double agent for the United States. He will, I expect, describe for us in detail the methods and approaches which the Soviets routinely use in an effort to obtain classified documents through the compromise of American personnel. His testimony will, I believe, underscore the extent and sophistication of the foreign hostile intelligence threat against American personnel, both domestically and abroad.

The Soviet's potential target, unfortunately, is an increasingly massive one, and this must be the focus of a great deal of our concern.

Today, more than 4 million Americans hold Government security clearances, including, astoundingly, more than 53-percent of Federal employees. More than 1½ million industry personnel are cleared. The latter figure alone has increased by over 44 percent since 1979.

Cleared personnel have potential access to an incredibly large amount of classified material. In testimony later this week, we will hear that today over 17 million Government secrets are housed by the Federal Government in one form or the other. If these were all stacked, they would equal the height of eight Washington Monuments.

During these hearings, the subcommittee will hear from those agencies responsible for performing those background investigations required prior to granting security clearances, including the Office of Personnel Management, the Defense Investigative Service and the FBI.

We also expect testimony from Government officials responsible for the adjudication or determination of whether a clearance should be granted based on these investigations, including representatives from the Department of Energy and the Department of Defense.

Finally, on the industry side, we will hear from Government contractors whose employees and security practices are subject to the Defense Industrial Program of the Department of Defense.

The testimony will, I believe, emphasize the fact that today's personnel security program is fragmented among many agencies, often resulting in inconsistency and unpredictability for the users of the program. The standards for background investigations vary, for instance, between the Office of Personnel Management and the Defense Investigative Service. Even within the Defense Department itself, we will learn that there are inconsistencies between background investigations for Government employees and those for contractors.

Adjudication of clearances hardly fairs better. In effect, each agency adjudicates its own cases, interpreting case law and governmental standards as it sees fit. Perhaps this is inevitable, but we will be exploring whether this is the best way to manage personnel security programs.

Testimony will also, I believe, relate other problems which continue to plague the personnel security program: limited investigative manpower in the face of a rapidly increasing workload; the inability of Government investigators to obtain needed information from State and local law enforcement agencies, and the reluctance of agencies to deny or revoke clearances except in the most flagrant cases.

We will also be looking at the ability of the Government to conduct personnel security investigations on immigrant aliens and recently naturalized citizens. Specifically, this investigation has suggested serious questions on the procedures used to clear former General Dynamics employee Panagiotis Takis Veliotis. Veliotis, a Greek shipbuilding executive with Canadian citizenship, was placed in charge of a highly classified military and nuclear propulsion program before fleeing the country in connection with his indictment in an alleged $2.7 million kickback scheme. We understand Mr. Veliotis was cleared despite inconsistent and unverifiable information uncovered in his background investigation. As a matter of fact, he was head of a shipyard for a period of months before he ever received his clearance. This shipyard was dealing with very highly classified information.

It is difficult enough to grant a security clearance for someone who has recently immigrated to our Nation. American investigators simply have great problems trying to conduct background inquiries in a foreign nation. It is especially difficult and sometimes impossible when the clearance is for someone from Communist nation or a closed society, like Iran.

One of the issues we will examine in our hearings is how the Pentagon can improve its background investigations on immigrant aliens and recently naturalized citizens. Our challenge is, indeed, a formidable challenge here, that is to balance the fact that we are a Nation of immigrants with our national security requirements, a very difficult balancing job.

For example, statistics provided by DOD show that in the defense industrial sector, 121 Soviet emigres have top secret clearances, and 1,349 have secret clearances.

Other defense contractor employees who are cleared or in the process of being cleared and who are immigrant aliens or recently naturalized citizens number 3,291 from the People's Republic of China; 1,555 from the Soviet Union; 1,225 from Poland; and 1,056 from Cuba; and all of these, of course, either have access now or will have access when cleared. If you can imagine the difficulty of checking background in this country, imagine a background check in a country behind the Iron Curtain. This is a very difficult problem.

In the area of the Defense Industrial Security Program, we will have the benefit of the recent report of the Department of Defense Industrial Review Committee. That report was requested for internal Defense Department purposes by General Richard Stilwell, who will be testifying before the subcommittee Thursday morning. That report has been a great help to our subcommittee, and, I think, has identified and proposed answers to some of the most perplexing problems. The Defense Department has provided the subcommittee with that report, and I will offer it as an exhibit for the record.

[The exhibit was marked "Exhibit No. 1" for reference purposes and may be found on p. 1113.]

Senator NUNN. During the course of the next few days, we will be discussing in full the findings and recommendations of that report, but I would now briefly mention just a couple of the report's highlights that are interesting as we begin our hearings:

Severe manpower shortages at the Defense Investigative Service in the face of an incredibly huge workload: requests for contractor clearances to DIS now run as high as 26,000 per month.

Given current DIS manpower, it would take the Investigative Service an entire decade to perform the 280,000 clearance re-investigations required for contractor personnel as of the end of 1984. One of the recurring themes that we have heard in the *Bell* case and other cases is the fact that re-investigations are just as important, and in many cases more important, than the initial investigation. When you have periods of 20 and 30 years going by where people are given access on a continuing basis with no update investigation, and you have that continuing because of the huge workload and the lack of capable and qualified personnel who are on the Federal payroll to carry out this workload, it becomes a nightmare-type operation.

The single largest category of industrial clearances are those 900,000 employees holding secret clearances. The report found current procedures for granting secret clearances, and I quote the report, "to be among the weakest aspects of the Industrial Personnel Security Program" and noted that today thousands of persons have access to secret materials based only on National Agency Checks conducted more than 20 years ago.

Despite manpower shortages, clearances are requested for a large number of contractor personnel who do not require access to classified information. The report cites plumbers, electricians and custodial personnel as common examples.

Of the 115,000 contractor personnel with top secret clearances, 90,000 to 95,000 do not have frequent access to top secret material, and 35,000 to 40,000 have never had access to top secret material, which raises the question, obviously, of whether we are, indeed, being requested as a Government to clear far more people than necessary.

I look forward to discussing those problems and possible solutions with the Government and the contractor witnesses during the next few days.

Finally, we will also have before us Christopher Boyce, now serving 68 years on Federal convictions of espionage, escape, and bank robbery. Mr. Boyce and his co-defendant, Mr. Daulton Lee, perhaps better known as "The Falcon and the Snowman," after the book and movie of the same name, were convicted for selling some of this country's most highly guarded secrets to the Soviet KGB. As a former contractor employee who, at the time, held numerous high-level clearances, Mr. Boyce's testimony will, I believe, vividly demonstrate how the lack of adequate security measures can substantially heighten our vulnerability as a Nation to espionage.

Representatives of Mr. Boyce's former employer, TRW, will, for the first time, publicly testify on the lessons they have learned from that case and the steps they have taken to avoid repetition, as will two other defense contractors victimized by espionage—Hughes Aircraft in the case of William Holden Bell, and Systems Control Technology in the case of James Harper and Ruby Schuler.

Again, Chairman Roth will be here in few minutes, but I want to thank him and his entire staff for their excellent cooperation in these hearings and investigation which has been underway for many months.

Our staff has prepared a series of exhibits, and I would like to have these exhibits received at this point in the hearing record and identified and numbered, beginning with Exhibit No. 2, Executive Order 10450. I would request these exhibits be printed in the appendix of these hearings or be made available in the files of the subcommittee. Without objection, this will be done.

[Exhibit No. 2 may be found in the files of the subcommittee. The other documents were marked Exhibits 3 through 11 for reference and may be found on pp. 1177–1310.]

Senator NUNN. Senator Gore, do you have an opening statement?

OPENING STATEMENT OF SENATOR GORE

Senator **Gore**. I have a brief one. I would like to commend you and Chairman Roth for convening these important and timely hearings. The threat of Soviet espionage is very real and simple logic dictates that we take all reasonable and prudent measures within our grasp to stem the unwanted flow of strategically critical technologies to our potential adversaries. This is precisely why so many of the cases we will examine in these hearings are so disturbing. It is unthinkable that a man who headed the development of two many weapons systems for General Dynamics would be allowed to do so without any clearances whatsoever, and even when this individual was eventually cleared, a layman could see that inconsistencies and gaps in the clearance record: At least one conviction was never even checked out, and on that basis, he should not have been cleared without a great deal more work, in any event.

It is equally dismaying that a situation such as the one at TRW could exist where a highly cleared employee could routinely spirit critical documents out of a security vault on an almost routine basis.

Moreover, this same individual seems to have received only a cursory background check.

Mr. Chairman, I am intent on finding out whatever dubious reasons the administration has for the apparent foot-dragging and bureaucratic wrangling that is currently taking place concerning our efforts to standardize and streamline the system of checking and clearing personnel.

The stakes are very high in America's effort to preserve our technological and strategic superiority. If there are gaps within our clearance system, it is within our power to close them. Therefore, there is no excuse for inaction and bureaucratic games.

Again, Mr. Chairman, I want to congratulate you and Chairman Roth on the superb effort in organizing and researching these hearings, and I am looking forward to participating in the proceedings.

Senator **Nunn**. Thank you, Senator Gore.

Our first witness is Mr. Bill W. Thurman, Deputy Director, National Security and International Affairs Division of the U.S. General Accounting Office.

Mr. Thurman, if you will come forward, I am sure you have associates with you. If any of them are going to testify, I ask you remain standing and take the oath. Those not testifying can go ahead and be seated.

Do each of you swear that the testimony you give before this subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. **Thurman**. I do.

Mr. **Boker**. I do.

Mr. **Reid**. I do.

Senator **Nunn**. We give oaths to all witnesses before this subcommittee, not just the General Accounting Office. [Laughter.]

We thank you for being here, Mr. Thurman. Your entire statement will be put in the record, if you choose to summarize.

TESTIMONY OF BILL W. THURMAN, DEPUTY DIRECTOR, NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION, GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY IRVING BOKER, ASSIGNMENT MANAGER, AND JAMES REID, GAO EVALUATOR

Mr. THURMAN. Thank you very much, Mr. Chairman. We appreciate the opportunity to appear before the subcommittee this morning and share with you the results of the work that we have undertaken over the past few years in this area.

If I could, I would like to introduce the people accompanying me today. Both of these gentlemen have had several years of experience working in the security area. Mr. Irving Boker is on my left; Mr. James Reid on my right. Mr. Boker serves as the assignment manager of GAO's work in this area.

I understand that you are pressed for time this morning and have quite a busy schedule. What I would like to do, if it is acceptable, is synopsize my statement. My complete statement was prepared with a view toward providing what we hope will be useful background information to the subcommittee and it includes a listing of GAO reports and recommendations and observations concerning personnel security and suitability. It includes a summary and status of principal recommendations that were in our reports issued between 1974 and 1984; a listing by agency of the number of Government and contractor employees with security clearances as of December 31, 1983; copies of Executive Orders 10450 and 10865 which govern personnel security in Government and industry, respectively, and, finally, a glossary of terms and acronyms relative to the Personnel Security Program.

I might mention, Mr. Chairman, that we would be more than happy to provide copies of all of the reports that are referred to in my statement if the subcommittee would find them of use.

Senator NUNN. Thank you, and we will remain in touch with you on that.

[At this point in the hearing, Senator Gore withdrew from the hearing room.]

[Letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive session hearings without a quorum of two Members for the administration of oaths and taking testimony in connection with hearings on "U.S. Government Personnel Security Program." These hearings are to be held on April 16, 17, and 18, 1985.

BILL ROTH,
Chairman.
SAM NUNN,
Ranking Minority Member.

Mr. THURMAN. At the risk of repetition, since you provided some statistics on security clearance, sir, in your opening statement, we do have some figures on security clearances throughout the Government. While the figures are more than 1 year old, we think they still provide some useful insight and perspective about the size of the program.

At the end of calendar year 1983, there were approximately 5,116,000 civilian and military personnel, of which 2,725,000, or about 53-percent, had security clearances. In addition, about 1,500,000 contractor employees had security clearances. That means that we are dealing with a universe here of roughly 4.2 million individuals with security clearances.

At the end of calendar year 1983, the Department of Defense accounted for 94-percent of the Government employees, and 87-percent of the contractor employees with security clearances. The Government performs well over a million personnel security investigations each year because of new employee hiring, changes in jobs, and retirements; military enlistments, promotions, and discharges; new programs; and periodic reinvestigations.

The Personnel Security Program, in our view, has improved in a number of ways during the past 10 years. Nevertheless, we believe that improvements are needed in six areas that we have identified through our work, and I will briefly highlight each of these areas.

The first one deals with the need for either legislation or a new Executive order. The second covers the subject of consistent standards for investigations and adjudications. The third deals with the need for centralized adjudication at the agency level.

Senator NUNN. Would you let me clarify now, definition-wide, so we can follow it? The investigation, the background report, is whatever degree of information is accumulated on a given individual, as I understand it. When you say the adjudication, that means that someone, either the investigative agency or, in most cases, some other agency, is taking the investigative report and they are deciding whether that individual deserves access to classified information based on those investigative facts?

Mr. THURMAN. That is correct, sir; that is the adjudicative process.

Senator NUNN. That is due-process appellate procedure. The employee himself or herself is not involved in that process.

Mr. THURMAN. Normally, they are not, sir. Normally, it is a review look by individuals who are charged with reaching a determination on whether or not the employee should be granted access to classified information.

Senator NUNN. In most cases, the people doing the investigations are not the ones who do the——

Mr. THURMAN [interposing]. That is correct, sir.

The fourth area that we believe requires some attention is the subject of continuous monitoring and periodic reinvestigation of employees who have received security clearances.

The fifth area deals with the need for timely investigations.

And, finally, the issue of how we get control over the number of requests for investigations that are being generated throughout the Government.

Executive Order 10450 entitled, "Security Requirements for Government Employment," as you mentioned, was issued in 1953 and is the basic authority for the Federal Government's Personnel Security Clearance Program. However, over the years, there has been a continuing debate and some uncertainty about the applicability of the order's provisions and their relationship to personnel suitability and security clearances.

In our two reports that were issued in the late 1970's—the December 1977 report and August 1979 report—we recommended to the Congress that it consolidate into one law the authority to investigate and judge or adjudicate the suitability of Federal employees, including the potential of employees in sensitive positions to impair national security.

We believe that legislation would be helpful primarily because it could address certain matters which cannot be dealt with by Executive order. For example, an Executive order cannot require local law enforcement authorities to provide information needed by the Government for security or suitability investigations. However, in the absence of legislation, we would support efforts to replace or revise Executive order 10450. Other studies, I might mention, have recommended, as you pointed out, replacement or revision of that order.

We believe that any changes to Executive order 10450 should be accompanied by the establishment of more consistent standards for investigations and adjudications.

In our 1979 report, we recommended that the Director of the Office of Personnel Management (OPM) work with other agencies to develop definitive standards for reporting costs and determining the scope of investigations. We concluded that once this was done, OPM, as part of its monitoring process, could make more accurate comparisons across agencies and determine the most effective program.

Our recent inquiries at several larger agencies indicated that inconsistent standards and procedures still exist. For example, DOD uses different procedures to grant secret clearances to Government and contractor personnel. A favorable national agency check and inquiries is required for Government personnel and only a favorable national agency check without the inquiries portion is required for industry employees.

A DOD official explained the rationale for this inconsistency in the following way: Executive order 10450, which governs only Federal civilian employees, requires the national agency check and inquiries. Executive order 10865, which covers the safeguarding of classified information in industry, does not have that requirement. This is one of the reasons that we believe the two Executive orders need to be rethought.

The establishment of consistent investigative and adjudicative standards alone cannot be fully effective without formal training programs for the investigators and adjudicators. They are, of course, a very important part of the Personnel Security Program.

Although useful guidance in personnel investigations and adjudications is available, we believe that personnel involved in these activities still need formal training governmentwide. Such training would provide greater assurance that the investigative and adjudicative processes are performed in a professional and consistent manner that protects the interests of the Government and the interests of the subjects of the investigations in a fair and equitable manner.

The Defense Investigative Service has a 4-week course at its Defense Security Institute in Richmond that is mandatory for all of its investigators, but few investigators from other agencies attend that course. OPM ran an adjudicator training class until 1983. OPM is now replacing that course as part of its establishment of three training courses. These courses, based on work done by a private contractor, are to be offered governmentwide. They will deal with investigations, security suitability, position sensitivity and adjudications. Such courses, in our view, could be useful to those investigators and adjudicators who have not had formal training or recent training in these areas.

Our third area of concern is the need for centralized adjudication at the agency level. In 1977, we recommended that OPM assign adjudicative responsibility for all sensitive positions to the employing agencies. This has been done. We recently surveyed six of the larger agencies—the Departments of Defense, Energy, Justice, State, Treasury, and the Postal Service. Excluding DOD, only the State Department said that it had a centralized adjudication process. The other four agencies were decentralized by bureau of field office, as the case might be.

Senator NUNN. In other words, you did not recommend—in fact, you recommended just the contrary, that there not be one central adjudication for the Government, but that the adjudication be in every agency.

Mr. THURMAN. That's correct.

Senator NUNN. You do recommend that at the agency level, the adjudication process be centralized and not dispersed all over the agency?

Mr. THURMAN. That is correct, sir. We found in some of the agencies, adjudication is a part-time function of the employees assigned to that duty. In our view, the centralized adjudication process within each agency provides greater assurance of uniformity and consistency in the application of standards and the criteria for granting access to national security information.

Within DOD, the Office of the Secretary of Defense is responsible for establishing security policy, and current regulations require that heads of the military services, to the extent practicable, establish a single adjudication facility.

The Army and the Air Force have complied with this instruction. The Navy has a centralized adjudication process for civilian personnel, but not for military personnel.

In May 1983, we, like others before us and others since, recommended that the Navy centralize the adjudication activity for its 3,000 commands and over 500,000 military personnel.

Senator NUNN. How many different areas of the Navy are involved in adjudication? Is that done base by base or ship by ship? How do they adjudicate?

Mr. THURMAN. Command by command.

Senator NUNN. For instance?

Mr. BOKER. It could be either way, by base or by ship, depending on location.

Senator NUNN. So some Navy ships do their own adjudicating?

Mr. BOKER. Yes, sir.

Senator NUNN. Sometimes the Atlantic Command or the Pacific Command?

Mr. BOKER. Yes, sir; that's correct.

Mr. **THURMAN**. The Navy has not responded, as of this date, to our recommendations.

Senator **NUNN**. When was that recommendation?

Mr. **THURMAN**. That recommendation was made in May 1983.

Senator **NUNN**. 1983.

Mr. **THURMAN**. Yes, sir. Monitoring previously cleared individuals to ensure that their access to classified information remains in the best interest of national security is, or should be, a continuing process. Policies and procedures for providing that assurance differ among the agencies. Government agencies and contractors need to continuously monitor cleared employees to detect those individuals with emotional, alcohol or drug-related or severe financial problems who may pose a threat to national security.

DOD requires its contractors operating some 14,000 cleared facilities that may have access to classified information to report any adverse information about an employee with a security clearance. This is a formalized reporting process with the reports being sent to the Defense Industrial Security Clearance Office, which is the central adjudication facility for contractor employees.

DOD regulations covering military and civilian personnel require the immediate reporting of adverse information by the most expeditious means possible to the commander or security officer of the organization to which the subject individual is assigned.

OPM has not established a similar adverse reporting requirement for all agencies, although some of the agencies may have established such a requirement on their own.

One of the other continuing problems that we have observed in the personnel security programs is getting investigations completed in a timely manner. Delays in the processing of security clearances result in significant cost to the Government. In our September 1981 report, we identified some of the causes and problems associated with the delayed processing of clearances.

In May 1981, DOD was processing top secret clearances for contractor employees on an average of 220 days, well above its standard of 90 days. Secret clearances for contractor employees were being processed in an average of 103 days, substantially above the 30-day standard.

We estimated that the lost productivity cost for contractor employees awaiting clearances, who could not have access to classified information without the appropriate clearance, could run as high as $340 million in fiscal year 1982.

Senator **NUNN**. $340 million in lost productivity?

Mr. **THURMAN**. Yes, sir.

Senator **NUNN**. In what area, just the Department of Defense?

Mr. **THURMAN**. Yes; that deals strictly with DOD.

Senator **NUNN**. Is that military and civilian?

Mr. **THURMAN**. That deals strictly with contractors.

Senator **NUNN**. Strictly with contractors. $340 million.

Mr. **THURMAN**. Yes, sir.

Senator **NUNN**. Have you tried to project that lost productivity with other agencies, including those investigated by OPM?

Mr. **THURMAN**. No, sir; we have not.

Senator **NUNN**. Is there any way that you could project that kind of lost productivity?

Mr. **Boker**. We can predict it for the military. DOD civilian and military personnel came out to about $580 million.

Senator **Nunn**. Per year?

Mr. **Boker**. Per year.

Senator **Nunn**. Military and——

Mr. **Boker** [interposing]. Civilian.

Senator **Nunn**. Includes contractor?

Mr. **Boker**. No, without contractor personnel.

Senator **Nunn**. $350 million, including contractors. Add the $350 million to the approximately $500 million DOD civilian and military, giving $850 million a year in lost productivity within the Defense Department and the contractor community.

Mr. **Thurman**. Yes, sir.

Senator **Nunn**. Almost a billion dollars.

Mr. **Thurman**. Yes, sir. That's a rough order of magnitude.

Senator **Nunn**. I understand.

Mr. **Thurman**. There really is no precise way to identify——

Senator **Nunn** [interposing]. Most of the time they go ahead and do the hiring, but just don't allow access?

Mr. **Thurman**. That's correct.

Senator **Nunn**. Are there other cases where they don't hire at all until they get security clearance, or most of the time do they hire first and deny access?

Mr. **Boker**. In industry, you have to hire an employee first and then submit a request for a clearance. So the employee is waiting around for the clearance to come through in order to work. There are a few exceptions, but they are rare, and the same is true with civilian employment in Government. They can hire some people without the required investigations, but those are rare instances.

Senator **Nunn**. Have you talked to anybody in the Office of Management and Budget about this in terms of personnel allocations? Have you had any dialog with them as to whether they might add more people and, thereby, save an awful lot of lost productivity?

Mr. **Thurman**. There has been, Senator, some improvement. The numbers I was citing to you were in our September 1981 report.

Senator **Nunn**. 1981.

Mr. **Thurman**. Yes, sir.

Senator **Nunn**. Covering what period?

Mr. **Thurman**. The estimate covered fiscal year 1982, but we supported a DOD request for additional personnel to be assigned to the Defense Investigative Service and there has been improvement in the amount of time taken to clear the employees.

[At this point in the hearing, Senator Gore entered the hearing room.]

Mr. **Thurman**. In fact, by August 1984, after DOD hired additional investigators, the average processing time for top secret and secret clearances for contractor employees was reduced to 82 and 51 days, respectively. However, continuing increases in the number of requests for investigations and periodic reinvestigations are causing delays and increasing the time for processing clearances.

In January 1985, the average processing time for top secret and secret clearances for contractor employees had increased to 114 and 63 days, respectively.

For several years, OPM has experienced similar delays in processing the investigations that are a prerequisite for the granting of security clearances. In many cases, the Government cannot hire or place an individual in a sensitive position until a favorable investigation is completed.

In January 1985, the Department of Energy, the largest user of OPM, told us that the average processing time for background investigations was 217 days, or about 7 months. The State Department said that when it started using OPM for background investigations 3 years ago, the agreed turnaround time was 60 days. However, after the cases started taking 6 months, State began to conduct its own investigations using personal service contracts with FBI agents.

The last item I would like to briefly cover this morning involves the need to control the number of requests for the investigations that are required to grant security clearances.

Our experience with this problem has been limited to DOD and contractor personnel. Some contractors said that it was possible to circumvent the system and that they were requesting more investigations than they needed. Two of the contractors who acknowledged requesting a few more investigations than they required said that delays by DOD in completing investigations forced them into their somewhat untenable situation. If they received a new contract or needed additional employees for an existing contract, they could transfer appropriately cleared employees from other contracts; they could hire other contractors' employees who already had the needed clearances, which is costly, or they could submit a request in anticipation of need.

Audit reports by the military services also have identified situations where an excessive number of security clearances were being requested for military personnel. DOD has recognized the problem and has considered a number of options to try and control the proliferation of security clearances, such as authorizing a specific number of clearances for each major defense component and/or charging each component and its constituent contractors for each investigation requested.

DOD has also emphasized to its military commanders and program managers their responsibility to keep clearance requests to an absolute minimum.

Mr. Chairman, that is, I'm afraid, a not-too-brief synopsis of my complete statement. We will be pleased to respond to any questions that you might have.

Senator NUNN. We have some questions we will ask and others we will ask you for the record in the interest of time here.

One of the things I wanted to try to establish was the difference in the various agencies in the efficiency now. You went into this in some detail. Let me see if I have got the correct interpretation.

Did you try to compare the Defense Investigative Service to the Office of Personnel Management in terms of time, in terms of cost per investigation and in terms of method? How far did you go in making this comparison?

Mr. THURMAN. We have some limited information on that subject. There are some variations that we have observed during our work. Perhaps Mr. Boker may want to expand on my answer here.

But the Defense Investigative Service typically tries to come to closure on any conflicting information that is obtained as part of the investigative process.

OPM tends to leave resolve differences, conflicting items open and leaves it up to the agency to. That is one distinction.

Senator NUNN. Does that mean that the Defense Investigative Service does a more thorough job than the Office of Personnel Management in their checks; is that a fair deduction or is that taking it too far?

Mr. BOKER. More complete as opposed to thorough.

Senator NUNN. How would you say it then?

Mr. BOKER. A complete job; they complete the entire job, whereas the OPM may stop short of resolving differences that come up. I don't know if it is a question of thoroughness or not.

Senator NUNN. DIS is more complete and OPM is more open-ended?

Mr. BOKER. That's about the size of it.

Senator NUNN. What about the cost? Do you have any kind of cost comparison between the Defense Investigative Service——

Mr. THURMAN [interposing]. I can share with you our own experience within the General Accounting Office. I am not sure we have any throughout the Government. Our experience within GAO has been the cost of the DIS investigations is less than the cost of OPM's investigations.

Senator NUNN. For instance, do you have a number?

Mr. BOKER. Yes, we do. OPM is charging us $1,375 for a background investigation. Based upon several studies of security in GAO, including one by the FBI, it was recommended that we look for other sources. We checked with DIS, and we are getting the same background investigation for $500, and we are getting it done in less than half the time.

Senator NUNN. So you are getting a more complete investigation from Defense Investigative Service in less than half the time for about a third of the money?

Mr. BOKER. That's right.

Senator NUNN. As compared to OPM. Is there an explanation for those disparities?

Mr. BOKER. Well, I believe that DIS operates on a lower overhead cost than OPM does. OPM has a revolving fund in which they have to recover costs. DIS does not have that problem.

Senator NUNN. Is that because somebody else is absorbing DIS's cost? Is this a true cost comparison or is there some other part of the Defense Department absorbing a lot of those costs?

Mr. BOKER. I believe DIS's costs are based on its own component cost, without an overhead charge for the rest of the Department, such as the costs of the Office of the Secretary of Defense or any of the supporting components, whereas OPM has a very close control over its costs, and they have to recover whatever it costs them. This is by law.

Another factor is the volume. DIS does so many more investigations that it becomes cheaper.

Senator NUNN. Well, is there a governmental reason to separate these, or should the Government and the taxpayers be looking to the most efficient way to handle this? Is there a reason for having several different agencies doing the investigation?

Mr. **Thurman**. One of the recommendations that we have made, Senator Nunn, is that Government wide cost data be collected on the investigative process. If comparable data was available we would be in a position to make those kind of judgments.

Senator **Nunn**. You are saying you haven't done a thorough enough analysis to make definite policy recommendations?

Mr. **Boker**. I believe the problem is that many of the agencies do not collect their costs—DIS does and OPM, but the other agencies do not accumulate costs, so we cannot compare the Department of State or the Treasury Department or other agencies that do their own.

I would like to add one more thing to the earlier question on the difference in cost between OPM and DIS. OPM uses a long form for their background investigation in which they include all narrative on any interviews with people in the investigation. DIS, on the other hand, uses a short form; only negative information is put down. This is a tremendous timesaver which I understand OPM is now considering implementing.

Senator **Nunn**. Has anybody asked you, as the General Accounting Office, to undertake such an analysis, or do you think that will be done by the agencies themselves? How are you suggesting it be done?

Mr. **Thurman**. We had suggested, Senator, in our earlier work that the agencies begin to put in place, under OPM's leadership, a system for collecting the kind of data that we are discussing here.

We still believe that is an appropriate course of action. There seems to be in this whole area a lack of information and data on such issues as cost, the number of security clearances denied, revoked, and so forth.

For example, it's our understanding that within the Department of Defense, there is no total system for aggregating a complete picture on the revocations or denials of security clearances that would enable comparisons to be made.

Senator **Nunn**. The number I have seen on denials are very, very, very low.

Mr. **Thurman**. Yes, sir.

Senator **Nunn**. We will get into that a little bit later. What you are saying is that GAO, as a user, without having done a policy-type analysis, is getting a lot cheaper, a lot quicker and a more complete service from DIS than from OPM?

Mr. **Thurman**. Yes, sir; I think that is true.

Senator **Nunn**. Does GAO have a choice? How do you decide who does your background investigations? Is it based on classification? Obviously, you would want to go with DIS, wouldn't you, most of the time?

Mr. **Thurman**. Yes. Our decision to use DIS, as Mr. Boker stated earlier, was based on a series of studies that were done 3 or 4 years ago.

Senator **Nunn**. You have that choice, though?

Mr. **Thurman**. Yes, sir.

Senator **Nunn**. Does the policy permit any agency to choose——

Mr. **Boker** [interposing]. No.

Senator Nunn. I thought there were definite types of cases that OPM has to handle.

Mr. Boker. You are correct in that assumption. We have two things going for us. No. 1, we are part of the legislative branch. No. 2, we have our own Personnel Act which was passed 2 years back which gives us authority.

Senator Nunn. Let's take another agency that is not in the legislative branch, not part of it. Do they have a choice as to who does their background investigation, or are most of them decided by law?

Mr. Boker. That varies. If it is excepted service——

Senator Nunn [interposing]. Excepted what?

Mr. Boker. Excepted service. That would be FBI, Secret Service, Bureau of Customs, perhaps the CIA, I think I mentioned, and several others, either by law or by some other means have the authority to go elsewhere.

[At this point in the hearing, Senators Roth and Chiles entered the hearing room.]

Senator Nunn. Just a couple more questions, and I will defer to Chairman Roth and then my colleagues.

On page 2 of your testimony, you state that program improvements are needed in six areas. National Security Decisions Directive 84, issued in March 1983, authorized an interagency study of the Federal Personnel Security Program.

Have you reviewed that study?

Mr. Thurman. That study, sir, has not been completed.

As you mentioned, the directions for it came from the National Security Directive. It requests the Attorney General to head an interagency task force and examine the applicability and viability of the Executive orders and the statutes in this whole arena.

Senator Nunn. What has happened to this study?

Mr. Thurman. It is our understanding that the study group in May of 1984 submitted several policy issues to the National Security Council for resolution before proceeding to conclusion of their study.

Senator Nunn. When did they submit that to the National Security Council?

Mr. Thurman. May of 1984.

Senator Nunn. What has happened since then?

Mr. Thurman. We were advised, as of last week, that the National Security Council is still considering the issues that were presented to it by the interagency group.

Senator Nunn. So, basically, the National Security Council asked for the study, designated an interagency group, got a series of questions back from the interagency group in May of 1984 and has not responded as of April 1985?

Mr. Thurman. Yes, sir; that's our understanding.

Senator Nunn. Does that mean it is dropped from the agenda? Does that mean somebody——

Mr. Thurman [interposing]. No; I don't think it has been dropped.

Senator Nunn. Really working on it? Having a difficult time?

Mr. Thurman. As I understand the status of it, we have spoken to some of the people who have participated in the interagency group and they are awaiting a decision from the National Security Council before proceeding with the——

Senator NUNN [interposing]. Is somebody physically working over at the National Security Council?

Mr. THURMAN. I don't think we know, sir.

Mr. BOKER. It is classified.

Senator NUNN. Do you have any suspicions you want to share with us?

One other question. Re-investigation; there was a moratorium, you say in your statement, on DOD re-investigations which has been lifted. Can you tell us about the re-investigative procedures and how effective re-investigations are?

Mr. THURMAN. We have not evaluated DOD's re-investigation program. Therefore, we are not in a position to comment on its effectiveness. However, we have had some discussions with certain DOD officials and the program, as described to us, appears to be an improvement. Each of the DOD components was given an allocation for re-investigations and each component was charged with responsibility for developing its own priorities re-investigations.

It is our understanding that the people who would be subject to re-investigation would be those in the more sensitive positions. However, with an allocation of 40,000 re-investigations, which is what we were talking about, contrasted with the number of top secret clearances and SCI accesses—something on the order of half a million—it is clear that DIS faces a very formidable task in getting current on the re-investigation process.

Senator NUNN. Do you all have any observations about the sheer numbers of people that are being requested for clearance? Are we talking about a situation that has just gotten out of hand, or do we really need to have—how many people total? Do 4 million people overall have to be cleared?

Mr. THURMAN. Yes, sir. About 4.2 million people, including contractors, is about what we have cleared throughout the Government.

Senator NUNN. Do we really need 4.2 million people in this country cleared for classified information?

Mr. THURMAN. You are asking a very, very difficult question. Maybe I can duck it and share with you some statistics. Between 1982——

Senator NUNN [interposing]. And that figure doesn't include members of the news media, does it?

Mr. THURMAN. No, sir, there was a growth in the number of security clearances granted of about 7.5-percent between 1982 and 1983. We don't have in our possession the more current numbers, but we are informed by DIS that their workload seems to be growing. As I pointed out in my statement one of the issues that is of continuing concern in this whole area is how one comes to grips with screening out those people that have a legitimate need and requirement for security clearance versus those that do not, and we have seen examples in our work of too many requests for security clearances.

Putting a number on that, Senator, is very, very difficult.

[At this point in the hearing, Senator Chiles withdrew from the hearing room.]

Senator **Nunn**. Let's say there could be two great problems here, both may be great problems. One may have a partial answer and one not at all. One is do we have entirely too much classified information? That is a legitimate question. It seems to me that may have to precede the question of whether we have too many people cleared. That is one question.

The second question is do we have too many people cleared? I know you can't quantify an answer to either of those. If you had to address which of those two problems is of the greatest magnitude based on your experience, what would you give? I am asking for your personal opinion, not speaking for GAO. I ask Mr. Boker also.

Mr. **Thurman**. Fine; I can share with you my own impressions from the classified material that I have seen in carrying out my present responsibilities.

I think it is fair to say, from the classified documents that I have seen, that I would consider most of those classifications to be justified and in the national interest. GAO issues, as you know, a number of classified reports each year. Our people working in the National Security and International Affairs Division deal quite extensively with classified information in carrying out our work. I see a lot of it.

I have not detected, in my own personal judgment, what I would consider to be an overclassification problem. That is a highly subjective answer.

Senator **Nunn**. I understand that. Would you then conclude the numbers of people that are classified may be the larger problem?

Mr. **Thurman**. Yes, sir, from our work, I think of the two, that would probably be the larger problem.

Senator **Nunn**. Mr. Boker, what is your personal judgment on that?

Mr. **Boker**. Well, we have been working in the area over 7 years. Our perspective is quite different from Mr. Thurman's. He sees the more sensitive areas. From what we have seen, I would say that there is much information out there that is classified that should not be classified. Everything is just marked "secret" and there are many things there that have no need to be secret. We are not experts in classification management or marking. Some information just looked like information that was readily available elsewhere and didn't have to be classified.

I believe that figure of 17 million classified documents, mentioned earlier may be rather low. I think there are probably that many in industry, at least there were 3 or 4 years ago. That figure does not include the classified documents within the government.

I would say that in many cases, people are given security clearances for operational convenience as opposed to need. This has been a recurring theme we have seen in DOD internal reports and talking to people.

Senator **Nunn**. So you say both of those problems: there may be too many people and too much classified information.

Mr. **Boker**. Yes, sir.

Senator **Nunn**. If you tried to classify too much, you end up having less secrets in terms of the final analysis.

Mr. **Boker**. Definitely.

Senator NUNN. By trying to protect everything, you protect nothing.

Mr. BOKER. That is absolutely correct.

Senator NUNN. Chairman Roth, I have already gone into considerable praise of you and the majority for your total cooperation in this set of hearings in my opening statement. We heard from GAO. I asked my questions. Senator Gore gave an opening statement. At this stage, I will turn the gavel back over to you as the Chairman and thank you for your cooperation, and you proceed from here. I know we would love to have your opening statement.

OPENING STATEMENT OF CHAIRMAN ROTH

Chairman ROTH [presiding]. Thank you, Senator Nunn. I apologize for being late. I, too, want to compliment you and the minority staff for doing what I think is an outstanding job on a critically important problem. I really don't think we can overemphasize the importance of these investigations.

Our Nation's first defense against hostile foreign intelligence agents is our people. It is people, not machines, who must safeguard our technology and protect our military secrets.

[At this point in the hearing, Senator Chiles entered the hearing room.]

Chairman ROTH. Padlocks, bolts, codes cannot keep these items safe from the intrusive designs of our enemy, though it is critically important that we have a strong, well-managed and efficient program to ensure that those with access to our Nation's secrets are trustworthy and not subject to blackmail and compromise.

Without objection, I will include my full statement so that we can continue with the hearings.

[The statement referred to follows:]

PREPARED STATEMENT OF CHAIRMAN ROTH

Beginning today, the Permanent Subcommittee on Investigations examines the critical link in our system of safeguards for classified materials and projects in the federal government.

Under the able leadership of Senator Sam Nunn, the minority staff, with the full support of the majority, has conducted an exhaustive review of the policies and procedures by which background investigations are conducted and clearances granted for persons and facilities to which sensitive materials are entrusted. The critical importance of these investigations cannot be over emphasized. Our nation's first defense against hostile foreign intelligence agents is our people. It is people, not machines, who must safeguard our technology and protect our military secrets. Padlocks, vaults, and codes can not alone keep these items safe from the intrusive designs of our enemies. We must also have a strong, well managed, and efficient program to ensure that those with access to our nation's secrets are trustworthy and not subject to blackmail and compromise.

That all important task falls to the agencies and persons who are designated to conduct and adjudicate background security investigations. With responsibility for literally hundreds of thousands of cleared personnel and facilities, the task is awesome. But failure can be disastrous. The presence of one "mole", one spy, in a sensitive program can cost not only millions of dollars to recover from but, more importantly, can jeopardize the lives of our people overseas and our very well being at home. The impact on our security by the failure to identify potential risks will clearly be demonstrated during the course of these hearings and should give us new understanding of the manipulative approach our enemies use to compromise American citizens to their will.

Senator Nunn, I commend you and your excellent staff for the hard work and superior effort on this important investigation.

Chairman ROTH. Senator Gore, do you have any questions?

Senator GORE. I have not asked questions.

Chairman ROTH. Go ahead.

Senator GORE. I just have a few, Mr. Chairman. I think we are all familiar with the cartoon image of a mindless bureaucrat stamping documents "Secret" on an assembly line basis. What we are seeing here is evidence that other bureaucrats are using another assembly line to give out secret security clearances in an indiscriminate fashion.

Your summary, Mr. Thurman, shows that there is no consistency whatsoever among the Federal agencies that have responsibility in this area. Your studies also show that these procedures are governed by a patchwork of Executive orders over 20 years old, and what this Nation needs is legislation or a comprehensive new Executive order providing sensible procedures on a consistent basis; would you agree with that?

Mr. THURMAN. Yes, sir, I would basically agree with that summary. There are, Senator Gore, some practices which generally tend to fall into the same framework between Federal agencies, but your basic synopsis is correct.

Senator GORE. Well, I would hope, Mr. Chairman, as we go through these hearings, we would keep in mind the recommendations of GAO and look at the possibility of legislation at the conclusion of these hearings because, frankly, I am not sanguine about the possibility of a comprehensive Executive order in this area. I think it would probably require legislation.

Now, is it fair to say as well that the number of individuals with security clearances have continued to go up since the figures that you cite were compiled? You give the number at the end of 1983.

Mr. THURMAN. We give the number of clearances at the end of 1983. We don't have any more current information. However, there was growth on the order of about 7.5 percent between 1982 and 1983. From our discussions with people in the field, it is our impression that their workload is increasing, which would suggest that probably the numbers are rising.

Senator GORE. So we have a security clearance inflation problem. Are NAC's, national agency check, or NACIs effective at all? One reason I ask is they don't seem to include questions on criminal justice information obtained from local law enforcement agencies; is that correct?

Mr. THURMAN. The national agency check focuses on gathering information that is available at the Federal level from Federal law enforcement activities.

With regard to the first part of your question, there are mixed views on that. Many personnel security specialists feel that while quite often the national agency checks do not disclose any derogatory information that they do on occasion disclose some information that makes them worthwhile.

Senator GORE. Well, now, OPM handles NACI's for the agencies, do they not?

Mr. THURMAN. Yes, sir.

Senator GORE. But OPM does not do any followup in cases where there is an inconsistency in the information obtained. If that is correct, doesn't that create a problem for the agencies?

Mr. THURMAN. We understand, from talking to some of the officials in the Federal agencies, that that practice has caused some difficulties and some concerns.

Senator GORE. Does DIS also leave such inconsistencies dangling?

Mr. THURMAN. DIS attempts to come to closure on any inconsistencies that are identified in their investigation.

Senator GORE. Well, what is wrong with OPM?

Mr. BOKER. I believe that there is a resource problem. The NACI, national agency check and inquiries, is done for free for Government agencies. There is no charge for it. If a NACI warrants an investigation to resolve a discrepancy, the agency would have to pay for it and that has been one problem. Agencies do not want to pay, and I believe OPM is short on resources.

Senator GORE. So we must skimp on the national security instead?

Mr. BOKER. That's about it, I'm afraid, unless the agency itself wants to conduct an investigation. Some agencies do have resources and may resolve the problems. If there is a discrepancy, the agency may confront the employee and ask about it or may conduct its own investigation, but that will vary among agencies.

Senator GORE. I am certainly looking forward to questioning the head of OPM and all of the other witnesses during these 3 days of hearings. I also brag on the subcommittee. I think this is a tremendous investigation that has needed to be done for a long time.

I might just say in closing, Senator Nunn and Mr. Chairman, last year on the House side, we had some hearings on FEMA. One of the things we found just in passing—the investigation was about something entirely different—the man in charge of physical security for the entire Federal Emergency Management Agency, was given a top secret clearance, even though he is a convicted felon. That peaked my interest in this whole procedure, and now looking at the tremendous work the staff has done in preparing for this hearing, I see a great need for either legislation or comprehensive Executive order, and I would lean toward legislation. Thank you.

Senator NUNN. I would share that view. I think we are going to have legislation and an Executive order, and I think we are going to have extraordinary cooperation with the executive branch in this area. The scope of the problem is just unbelievable in terms of numbers involved. It makes you wonder how many espionage cases we have. We have the FBI testifying about the record number being prosecuted. It makes you wonder about the ones that are actually going on. With these numbers involved, you have to have serious questions.

I have forgotten the ratio they use of the people caught for bringing drugs into the country. Senator Chiles probably knows that.

Senator CHILES. Ten to 20 percent.

Senator NUNN. About 90 percent getting through. It makes you wonder if there is a factor like that here, maybe more, when you consider the number of people who are cleared.

Senator CHILES. Your sergeant is going to testify. He had been operating for 10 years. That gives you some pause for thought that the procedure would allow him to operate for 10 years.

Senator **Nunn**. In this case, he was one of the good guys, but we are going to hear the scope of the problem later on this week certainly in detail.

Chairman **Roth**. Senator Chiles?

Senator **Chiles**. Mr. Chairman, I have a short opening statement I would like to submit for the record.

OPENING STATEMENT OF SENATOR CHILES

Senator **Chiles**. Primarily, I want to commend the Senator from Georgia for his diligence in directing a thorough investigation on this issue. It strikes at the very heart of our national security. I want to assure him and you, Mr. Chairman, of my support for this investigative effort. I would like to ask Mr. Thurman—I don't know whether this has been within the scope of what you were looking at—we give, it seems, extraordinary license to the Russians. For example, to travel our country, to be free to get out to the countryside and make any and all contacts they wish to make.

My understanding is, we are much more restricted in that way in what happens over there. Do you have any idea of how that affects this problem, the fact that we do allow them the freedom to contact, to travel, to go to all of these places? It certainly allows them to set up their liaisons. We get estimates of how many espionage agents they actually have sent to this country through the UN personnel, through their diplomatic personnel, through business and other people that are travelling.

Mr. **Thurman**. Senator Chiles, we really don't have any information that directly addresses your question. I would suggest, perhaps that some of the ensuing witnesses that the subcommittee will hear from will be able to respond with a little more informed judgment on that particular question.

Senator **Chiles**. That is all, Mr. Chairman.

Chairman **Roth**. Mr. Rinzel

Mr. **Rinzel**. Mr. Thurman, you indicated in your testimony that some of the problems resulting in this area are the result of backlogs in investigations and an increasing number of investigations.

[At this point in the hearing, Senator Chiles withdrew from the hearing room.]

Mr. **Rinzel**. Given the fact that a very large number of these clearances are in the Defense Department and that the military budget has been increasing, which also causes an increase, of course, in the number of contractors that need to be cleared, would it make any sense to require that in the budget process itself that military projects requiring clearances include the cost of such security checks in that budget process?

Mr. **Thurman**. Quite honestly, I think I would respond similar to how I responded to Senator Chiles. I am not sure we are your best source for a judgment on that particular question. We do know that some of the things that DOD has thought about doing to try to control the number of security clearances that are being requested are ideas like a revolving fund or an industrial fund where commands or components would be required to pay for their investigations.

[At this point in the hearing, Senator Gore withdrew from the hearing room.]

Mr. **Thurman**. I am just not sure whether it would be practical to separate it as an individual line item on a particular program.

Mr. **Rinzel**. Isn't DIS now the stepchild of the Defense Department in that when they get additional workloads, they don't get additional money?

Mr. **Thurman**. Yes, that has happened in the past, as we pointed out, particularly in the early 1980's. The caseload, in relation to the number of people available, was just out of balance. So, yes, that has occurred in the past.

Recently, there has been, as you are aware, an increase in the number of DIS investigators used to handle the growing caseload, and that has had some degree of success, as shown by the declining number of days that are involved in completing investigations. However, more recently there has been an upswing again in terms of the number of calendar days required to complete an investigation.

Mr. **Boker**. There has been a question of identifying security costs in general, not just those involved with personnel security investigations, but the money spent on physical security and information security and that the disproportionate amount spent on personnel security compared with the safes, the locks, the bolts, the guards, fences, and what have you, when the biggest threat is from individuals, as opposed to the physical portion of the protection.

Mr. **Rinzel**. I have one other question. Senator Nunn asked you some questions about the overclassification of documents. What about projects? The Los Angeles Times ran a piece last week about black and white projects, classified an nonclassified, with the suggestion that there were too many projects that were black projects and that the costs, therefore, go up substantially for such projects. Would you have any view on that?

Mr. **Thurman**. This is purely, again, a personal view from my own knowledge of some of the so-called black programs and projects.

My general perception is that those classifications are justified. Bear in mind, I am talking about very anecdotal kinds of experiences here, but my general impression is that, from the ones that I have seen, the classifications are appropriate. That is my judgment. We did some work on special programs that Mr. Boker might want to talk about.

Mr. **Boker**. We have special access programs, and most of them involve contractors. So, we have special access contracts and there are about 5,000 or 6,000 of those contracts open or active. They involve special access requirements, special protection measures. There are quite a few out there. I think that most of them are properly justified. They have to be approved by the service secretary or the head of the component. A number of them are unauthorized—what we call carve out contracts—taken out of the Defense Investigative Service responsibility for inspection and oversight. There are a number of those. How many, we don't know, nor do many of the DOD components know. DOD is trying to get a handle on the situation, but it is a continuing problem, compounded by the fact that they want to maintain security. With so many employees in industry with only secret clearances based upon a national agency check, they have taken these projects and made them special access to really control the amount of access to the particular contract or project.

Mr. RINZEL. I don't have any further questions, Mr. Chairman.

Chairman ROTH. I just have one comment, and perhaps one question of you, Mr. Thurman. As I indicated in my opening statement, I think these are particularly important hearings which is a critical matter. One of my concerns in this area is the question of where do you draw the line? It is a question of delicate balance between overclassifying and underclassifying. It is an area that we in the Congress love because you can always criticize the executive branch from either direction. If you underclassify, there is always opportunity to be critical of that. On the other hand, my own feeling is that there is a tendency to overclassify.

That is something that has existed as long as I have been in the Congress.

The safe thing for any executive is to overclassify to protect himself. The question is how do we draw that delicate line because a lot comes down to discretion, I gather. For example, if I understand what you said, Mr. Thurman, in your opinion, the overclassification is not that serious at the current time, whereas Mr. Boker would have a different conclusion.

Mr. THURMAN. Mr. Chairman, you are raising a very good question and not an easy one to answer. In part, I think our differences in perspective derive largely from where we sit. In the job I have in the General Accounting Office, I review most of the classified reports that we issue. These reports are an aggregation of many pieces of classified data, and as I look at the complete reports, it seems to me almost in every case, that the reports should be classified.

On the other hand, from Mr. Boker's perspective, when he is out actually examining individual documents a different conclusion can be drawn. As I think back to when I was examining documents, I saw cases where I would wonder whether the documents really needed to be classified, particularly when I saw the same information in Aviation Weekly or some other publication a few weeks later. Please excuse my interruption.

Chairman ROTH. I must confess, it always bothers me to go to some kind of briefing and be told how confidential it is and then read it in Time or Newsweek next week. But my real concern, and I know this is Senator Nunn's concern, is how do we draw that line in a responsible way; how do we establish that balance? There are those, for example, who consider home computers a critical matter for export controls and others strongly disagree with that. This comes down to a matter of some judgment.

I guess one of the questions I would like to ask you, are the problems we face today new or are they something that has been continuing down through the years? The size of the problem certainly must be greater because of the defense effort.

Mr. THURMAN. I would certainly share your view that this has been an issue in my 22 or 23 years in the Government, and I suspect it will continue to be one because there are judgment calls involved here.

In attempting to strike a balance, it is almost inevitable that one person's sensitive information which should be classified, will represent an unnecessary coverup to another person, much depends on the perspective that one brings to a particular item.

Chairman **Roth**. I think both of you are able, responsible men, but there is a difference of opinion.

Mr. **Thurman**. Yes.

Mr. **Boker**. There won't be for long. [Laughter.]

Chairman **Roth**. Thank you, gentlemen. We appreciate very much, as always, your helpful testimony.

[Mr. Thurman's prepared statement, with attachments, and responses to written questions follow:]

PREPARED STATEMENT OF BILL W. THURMAN

Mr. Chairman, Ranking Minority Member, and Members of the Subcommittee:

I appreciate the opportunity to appear before you this morning to discuss (1) some of the principal recommendations in our reports on personnel security clearances during the past 10 years; (2) the status of those recommendations; and (3) our current thoughts on some of the issues raised by those recommendations. With me is Irv Boker, who is our manager for the security area.

I would like to submit for the record, and as part of my prepared statement, (1) a listing of GAO reports containing recommendations and observations concerning personnel security and suitability; (2) a summary and status of principal recommendations from GAO reports from 1974 to 1984; (3) a listing, by agency, of the number of government and contractor employees with security clearances as of December 31, 1983; (4) copies of Executive Orders 10450 and 10865, which govern personnel security in government and industry, respectively; and (5) a glossary of terms and acronyms relative to the personnel security program. Copies of the GAO reports included in the listing can be furnished if the Subcommittee would like to have them.

The personnel security program has improved in a number of ways during the past 10 years. Nevertheless, we believe that improvements are still needed in the following six areas.

--Legislation or a new executive order,

--Consistent standards for investigations and adjudications,

--Centralized adjudication at the agency level,

--Continuous monitoring and periodic reinvestigation of cleared employees,

--Timely investigations, and

--Control of the number of requests for investigations.

Background

Since the first executive order was issued in 1940 prescribing policy and procedures for security classification, various orders have been issued defining the levels of classification. The current executive order, 12356, issued in April 1982, like several orders before it, prescribes three levels of classification--top secret, secret, and confidential--depending upon the level of sensitivity of the information and the potential damage that would result from its disclosure.

The type of security clearance an individual needs is determined by the classification level of the information to which the individual will have access. For example, if information is classified top secret, the individual must have a top secret clearance to be given access. However, having a top secret security clearance does not automatically give the individual the right of access to classified information. The overriding general rule is still "need to know." That is, the individual must have an official need to know or see the information.

Most government and industry employees with security clearances have either secret or top secret clearances. A secret clearance can be granted if a National Agency Check and Inquiries (NACI) produces no serious derogatory information. The National Agency Check (NAC) portion consists of searching the records of certain federal agencies such as the Office of Personnel Management (OPM) and the Departments of Defense, Justice, and State to determine the existence of any previous investigations or a criminal record and to verify citizenship and any military service. The inquiries portion involves sending written inquiries covering specific areas of the subject's background during the past 5 years or since the individual's 18th birthday, whichever is shorter. A top secret clearance requires the same information but, in addition, it requires a favorable background investigation which covers the same period. The background investigation, among other things, includes personal interviews with people who know the individual being investigated and a verification of his or her birthdate, education, and employment.

In addition to a regular security clearance, the intelligence agencies, including some components of the Department of Defense (DOD) involved in intelligence activities, require that a more extensive background investigation be conducted before an individual is granted access to intelligence information, methods, or sources. Such information is referred to as sensitive compartmented information (SCI). The minimum standards for the special background investigation are prescribed by the Director of Central Intelligence.

The latest figures that we have on security clearances are more than a year old, but they nevertheless are useful to provide some perspective about the size of the personnel security clearance program. At the end of calendar year 1983, there were approximately 5,116,000 civilian and military personnel, of which 2,725,000, or about 53 percent, had security clearances. The number of clearances increased about 7.5 percent from 1982. In addition, about 1,500,000 contractor employees have security clearances. That means about 4,200,000 individuals have security clearances. At the end of calendar year 1983, DOD accounted for 94 percent of the government employees and 87 percent of the contractor employees with security clearances.

Executive Order 10450 makes OPM responsible for conducting all competitive service investigations used in determining the suitability of individuals for government employment and as a basis for insuring that the employment of the individual is clearly consistent with the interests of national security. Some agencies, such as the Departments of Defense, State, and Treasury, are authorized by law, or agreement with OPM, to conduct investigations of competitive service positions. Excepted service positions, however, are not covered by Executive Order 10450 and agencies are free to use whatever means they choose to investigate applicants for these positions.

OPM and DOD, through the Defense Investigative Service (DIS), perform the majority of the personnel investigations made each year. These investigations are needed because of new employee hiring, changes in jobs, retirements; military enlistments, promotions and discharges; new programs; and periodic reinvestigations. In calendar year 1984 OPM performed 245,000 investigations, including a large but unknown number that involved investigations to determine suitability for government employment. During this same period, DIS performed 1,071,000 investigations involving DOD and industry personnel. Ten other agencies also performed personnel investigations on some or all of their employees last year. Some examples are the Department of State, Central Intelligence Agency, Federal Bureau of Investigation, and Secret Service.

Legislation or New Executive Order Needed

Executive Order 10450 entitled *Security Requirements for Government Employment*, issued April 27, 1953, is the basic authority for the federal government's personnel security clearance program. However, there has been a continuing debate over the applicability of the order's provisions concerning personnel suitability and security clearances. In our December 1977 and August 1979 reports, we recommended that the Congress consolidate into one law the authority to investigate and judge the suitability of federal employees, including the potential of employees in sensitive positions to impair national security.

We believe that legislation would be helpful primarily because it could address certain matters which cannot be dealt with by executive order. For example, an executive order cannot require local law enforcement authorities to provide information needed by the government for security or suitability investigations. However, in the absence of legislation, we would support efforts to replace or revise Executive Order 10450. Other studies have recommended replacement or revision of the order.

Need for Consistent Standards for Investigations and Adjudications

In our December 1977 and August 1979 reports, we identified the need for consistent standards for conducting investigations and adjudications. For example, in our 1979 report, we recommended that the Director of OPM work with other agencies to develop definitive standards for reporting costs and determining the scope of investigations. We concluded that, once this was done, OPM, as part of its monitoring process, could make more accurate comparisons across agencies and determine the most effective program.

Our recent inquiries at several larger agencies indicated that inconsistent standards and procedures still exist. For example, DOD uses different procedures to grant secret clearances to government and contractor personnel. A favorable NACI is required for government personnel, but only a favorable NAC is required for industry employees.

A DOD official explained the rationale for this inconsistency as follows. Executive Order 10450, which governs only federal employees, requires the NACI. Executive Order 10865, issued February 20, 1960, which pertains to safeguarding classified information in industry, does not require the NACI. In our opinion, this illustrates why the two executive orders need to be rethought.

Another inconsistency in DOD is that some individuals with secret clearances are provided access to information while others with top secret clearances, and a "need to know" are denied access. This inconsistency was pointed out in our February 1983 report on special access contracts awarded by DOD. DOD's special access programs are supported by several thousand special access contracts. These programs and supporting contracts are controlled by the military service or DOD component responsible for the programs. At the time of our review, some of these nonintelligence-related contracts were classified only at the secret level. However, in many cases, DIS inspectors, with top secret clearances, were unable to make periodic security inspections of the contracts in accordance with DOD's Industrial Security Program because of limited access requirements. On the other hand, of about 39,000 contractor employees who had been cleared for access to nonintelligence-related special access contracts, 13,500 had only secret clearances. Some of those employees with only secret clearances had access to contract information. It seems inconsistent to allow access for contractor employees whose clearances were based on only a NAC, while denying access to a DIS inspector with a top secret clearance based on a background investigation.

In defense of this practice, DOD stated that it believed that a program security officer, with program familiarity, is better equipped to make inspections than a DIS inspector would be. DOD also said that access by DIS inspectors would cause the number of individuals with access to proliferate beyond the minimum number of individuals necessary to meet the objectives of providing extra security protection.

As noted in our report, we believe that a knowledge of security requirements is required to make security inspections and that DIS inspectors, who must receive formal training before being allowed to make inspections, may be better qualified than a program security officer. Further, when the number of contractor employees with special access authorizations is at least 39,000, it does not seem unreasonable for a small number of DIS employees to have such access.

We believe that the establishment of consistent standards for investigations and adjudications can not be fully effective unless the investigators and adjudicators are properly trained. Although useful guidance on personnel investigations and adjudications is available, we believe that personnel involved in these activities still need formal training government-wide. Such training would provide greater assurance that the investigative and adjudicative processes are performed in a professional and consistent manner that protects the interests of the government and the interests of the subjects of the investigations in a fair and equitable manner.

DIS has a 4-week course at its Defense Security Institute in Richmond that is mandatory for all DIS investigators, but few investigators from other agencies attend. The Institute currently has no adjudication course. The intelligence agencies have a course on adjudicating cases involving access to SCI, and some of the agencies do send representatives to that course. OPM ran an adjudicator training class until 1983. OPM is now replacing that course as part of its establishment of three training courses. These courses, based on work done by a private contractor, are to be offered government-wide. The courses deal with investigations, security, suitability, position sensitivity, and adjudications. Such courses could be useful to those investigators and adjudicators who have not had formal training or recent training in these areas. We believe that there is a need for a government-wide training program for both groups.

Need for Centralized Adjudication at the Agency Level

In our December 1977 report, we recommended that OPM assign adjudicative responsibility for all sensitive positions, which includes security clearances, to the employing agencies. This has been done. We recently surveyed six of the larger agencies--the Departments of Defense, Energy, Justice, State, and Treasury, and the Postal Service. Excluding DOD, only the State Department said that it had a centralized adjudication process. The other four agencies were decentralized by bureau or field office, as the case may be. At some of the agencies, adjudication is a part-time function of the employees assigned that duty.

Centralized adjudication provides uniformity and consistency in the application of standards and criteria for granting access to national security information. Since full-time adjudicators spend all, or a significant part of their time performing that function, they become more proficient, which means that fewer adjudicators are required. Centralization also means that adjudications can be more closely monitored to ensure that clearance decisions are uniformly made.

Centralized adjudication also reduces the potential for bias in an adjudicative decision. If the adjudication is made at a level low enough so that the adjudicator has personal knowledge of the individual, the decision might be influenced (either favorably or unfavorably) based on that knowledge rather than the criteria that are supposed to be used. As noted in a 1982 DOD report on its personnel security program, another factor that could influence an adjudicative decision, made at a lower level, is the immediacy of need for someone to occupy a position. Again, it is possible that the adjudicative decision could be influenced by that need rather than by strict adherence to the required criteria.

As far as the executive orders governing the protection of national security information are concerned, DOD is considered to be comprised of more than one department. The Office of the Secretary of Defense is responsible for establishing security policy throughout DOD, and current regulations require the heads of the military services, to the extent practicable, to establish a single adjudication facility. The Army and the Air Force have complied. All three services have their own centralized adjudication process for handling SCI accesses. The Navy has a centralized adjudication process for civilian personnel, but not for military personnel.

In May 1983, we, like others before us and others since, recommended that the Navy centralize the adjudication activity for its 3,000 commands and over 500 thousand military personnel. Because the adjudicative process is not centralized, data is not readily available on how many adjudications were performed in fiscal year 1984; however, there were 26,000 background investigations of Navy military personnel during that year by DIS. The Navy has not responded to our recommendation.

Need for Continuous Monitoring and Periodic Reinvestigation of Cleared Employees

The granting of security clearances to government or contractor employees is the first step in the protection of national security information. Monitoring previously cleared individuals to ensure that their access to classified information remains in the best interest of national security is, or should be, a continuing process. Policies and procedures for providing that assurance differ among agencies.

The Federal Personnel Manual, issued by OPM, which applies only to government employees, requires a reinvestigation every 5 years after an individual is placed in a position designated "special sensitive" or "critical sensitive". These terms are equivalent to an SCI access and top secret clearance, respectively.

In June 1981, DOD placed a moratorium on periodic reinvestigations for individuals with SCI access, because of the investigative backlog resulting from an increased number of initial investigations. In April 1983, because of improvements in the backlog and turnaround time, DOD resumed periodic reinvestigations for persons with SCI access and expanded the scope of its periodic reinvestigations of individuals with top secret clearances. To ensure that the periodic reinvestigations would not adversely impact the overall backlog and case completion time for all investigations, DOD established an annual quota of 40,000 periodic reinvestigations. With over 100,000 individuals with SCI access and about 500,000 with top secret clearances in DOD and industry, it may be several years before DIS can get the reinvestigation process back on schedule, considering its heavy work load of requests for new investigations.

The continuous monitoring of employees who have security clearances is also important. Government agencies and contractors need to pay close attention to employees with emotional, alcohol- or drug-related or severe financial problems. We have found that, when derogatory information on a individual is reported, agencies are reluctant to revoke security clearances because such revocation might be considered an adverse action. Agencies prefer to reassign the employee to a position that does not require a clearance.

DOD requires its contractors, operating some 14,000 cleared facilities that may have access to classified information, to report any adverse information about an employee with a security clearance. This is a formalized reporting process, with the reports being sent to the Defense Industrial Security Clearance Office, which is the central adjudication facility for contractor employees. During fiscal year 1984, the Clearance Office received 2,400 reports with adverse information and, based on these reports, suspended 24 clearances, on an interim basis, until the adverse information could be resolved.

DOD regulations covering military and civilian personnel require the immediate reporting of adverse information, by the most expeditious means possible, to the commander or security officer of the organization to which the subject individual is assigned.

OPM has not established a similar adverse reporting requirement for all agencies, although some may have established such a requirement.

Timely Investigations are a Significant Factor

Delays in the processing of security clearances result in significant costs to the government. In our September 1981 report, we identified some of the causes and problems associated with the delayed processing of clearances. In industry, a contractor is required to hire an employee before submitting a request for a security clearance. If the individual does not have a clearance, or is cleared at a level lower than what is needed for the job, the individual is not given access to the classified information for which the clearance is requested until the clearance request is processed favorably. In May 1981, DIS was processing top secret and secret clearances for contractor employees in an average of 220 and 103 days, respectively, well above its standard of 90 and 30 days, respectively.

Based on an earlier industry study that identifed the costs of the lost productivity of individuals awaiting clearances, and not being able to do the classified contract work for which they were hired, we estimated that such costs could have totaled about $340 million in fiscal year 1982. Using the industry study as a basis for DOD in-house costs, we estimated that such productivity losses within DOD for both civilian and military personnel could have run as high as $580 million a year.

On the basis of this work, we supported a DIS request for additional investigators to help reduce the backlog and processing time of clearance requests. Additional investigators were authorized, and the backlog and processing time were both reduced. By August 1984, the average processing time for top secret and secret clearances for contractor employees had been reduced to 82 and 51 days, respectively. However, continuing increases in the number of requests for investigations and periodic reinvestigations are causing delays and increasing the time for processing clearances. In January 1985, the average processing time for top secret and secret clearances for contractor employees had increased to 114 days and 63 days, respectively.

For several years, OPM has experienced similar delays in processing the investigations that are a prerequisite for the granting of security clearances. In many cases, the government cannot hire or place an individual in a sensitive position until a favorable investigation is completed. In January 1985, the Department of Energy, the largest user of OPM, told us that the average processing time for background investigations was 217 days, or about 7 months. The State Department said that when it started using OPM for background investigations 3 years ago, the agreed turnaround time was 60 days. However, after the cases started taking 6 months, State began to conduct its own investigations, using personal service contracts with ex-FBI agents. The Justice Department also told us that OPM investigations were being completed in about 6 months.

Need to Control the Number of Requests for Security Clearance Investigations

Excessive requests for security clearances is a contributing factor to backlogs and processing delays and the incurrence of unnecessary costs. In our February 1983 report, which pertained only to DOD special access contracts, we recommended that instructions be issued that would require DOD's advance approval of a contractor's nominee for a special background or regular background investigation. We also recommended that the DIS return to contractors any requests not containing the advance approval. DOD took steps to implement our recommendations.

Some contractors said that it was possible to circumvent the system and that they were submitting more requests than they needed. Two contractors who acknowledged requesting a few more special access authorizations than they needed said that delays by DOD in completing investigations forced them into an untenable situation. If they received a new contract or needed additional employees for an existing contract, they could transfer appropriately cleared employees from other contracts (which would delay that work), hire other contractors' employees who already had special access authorizations (which was costly), or submit requests in anticipation of need.

DOD officials have told us of cases where contractors' employees had security clearances that were in excess of the number needed to perform on classified contracts. Over the years, audit reports by the military services have identified situations where an excessive number of security clearances were being requested for military personnel. DOD recognizes the problem and has considered a number of options to control the proliferation of security clearances, such as authorizing a specific number of clearances to each major defense component, and charging each component and its constitutent contractors for each investigation requested. DOD has also emphasized to military commanders and program managers their responsibility to keep clearance requests to an absolute minimum.

- - - - -

This concludes my prepared statement. If you have any questions, we would be pleased to answer them.

GAO Reports Containing Recommendations and Observations Concerning Personnel Security and Suitability

Date	Number	Title
12/02/74	B-132376	Personnel Security Investigations: Inconsistent Standards and Procedures
12/16/77	FPCD-77-64	Proposals to Resolve Longstanding Problems in Investigations of Federal Employees
01/30/79	GGD-78-91	IRS Inspection Service Functions: Management Can Further Enhance Their Usefulness
08/31/79	FPCD-79-79	Costs of Federal Personnel Security Investigations Could and Should Be Cut
09/25/79	FPCD-79-92	Status of the Investigative Program
09/15/81	GGD-81-105	Faster Processing of DOD Personnel Security Clearances Could Avoid Millions in Losses
07/08/82	GAO/GGD-82-56	The Department of Justice Needs to Address the Problem of Two Personnel Investigations Being Conducted on All Bureau of Prisons Employees
10/07/82	GAO/GGD-83-15	Review of Department of Defense Investigation of Leak of Classified Information to The Washington Post
02/18/83	GAO/GGD-83-43	Further Improvements Needed in Department of Defense Oversight of Special Access (Carve-out) Contracts
05/18/83	GAO/GGD-83-66	Need for Central Adjudication Facility for Security Clearances for Navy Personnel
10/18/83	GAO/NSIAD 84-26	Effect of National Security Decision Directive-84, Safeguarding National Security Information
06/11/84	GAO/NSIAD 84-134	Polygraph and Prepublication Review Policies of Federal Agencies

Summary and Status of Principal Recommendations
From GAO Reports 1974-1984

			Status as of February 1985		
Report Number & Date	Recommendation	Implemented	Partially Implemented	Not Implemented	No Longer Applicable
B132376 12/2/74	We recommend that Civil Service Commission (CSC) (OPM)				
	--assume a more active role in providing direction and guidance regarding the classification procedure and the adjudication process.	X			
	--examine existing classification criteria to see if they are as ambiguous as agencies claim.	X			
	--consider the possibility of establishing a central adjudication body to review derogatory cases.				X
	--assume complete responsibility for the investigative function of all civil agencies.			X	
FPCD-77-64 12/16/77	We recommend that the Congress consolidate into one law the authority to investigate and judge the suitability of federal employees, including the potential of employees in sensitive positions to impair national security. The Congress should consider:			X	
	--Restrictions imposed on personnel investigations by other laws, such as the Privacy Act of 1974, and court decisions protecting individuals constitutional rights.				

Report Number & Date	Recommendation	Status as of February 1985 Implemented	Partially Implemented	Not Implemented	No Longer Applicable
	--Whether CSC (OPM) should investigate occupants of nonsensitive positions only to determine prior criminal conduct, leaving to employing agencies the responsibility for assessing applicants' efficiency.				
	--Need to define, in a manner acceptable to the courts, disloyal acts which should bar federal employment.				
	--Scope of investigation needed for the seven levels of security clearances granted federal employees.				
	--Whether there is a need in the legislation for provisions to aid CSC (OPM) in gathering local law enforcement information; e.g., reimbursing local law enforcement agencies for supplying information, receiving assistance from federal law enforcement agencies, or clarifying CSC's (OPM's) legal authority to have local arrest information.				
	We recommend that CSC (OPM):				
	--Establish criteria which will provide agencies clear instructions on how to classify positions into three categories based on whether the position duties would enable an occupant to have (1) a materially adverse effect on national security and/or a materially adverse effect on other national interests, (2) a materially adverse effect on agency operations, or (3) no materially adverse effect on agency or national interest.	X			
	--Assign more people to the review of agency classifications to bring about consistent use of the categories and thus appropriate investigations.		X		

Report Number & Date	Recommendation	Status as of February 1985			
		Implemented	Partially Implemented	Not Implemented	No Longer Applicable
	--Establish controls which insure that written inquiries are responded to and used for adjudication.		X		
	--Establish clear criteria for determining when cases should be further investigated to obtain complete and accurate information and to ascertain if a pattern of misconduct is continuing or if rehabilitation has been accomplished.		X		
	--Establish controls to prevent arbitrary reductions in the scope of investigations.			X	
	--Assume complete responsibility for adjudicating past conduct in making suitability determinations for occupants of nonsensitive positions and retain the investigative results.		X		
	--Assign adjudication responsibility for all sensitive positions to employing agencies.	X			
	--Establish criteria on the completeness, accuracy, and age of information which can be used by CSC (OPM) for adjudication or be disseminated to an employing agency for its adjudication. Also, restrict the collection of information to that which can be used.	X			
	--When needed to determine the qualifications of potential appointees, direct employing agencies to make appropriate inquiries of prior employment and educational sources.			X	

Report Number & Date	Recommendation	Status as of February 1985			
		Implemented	Partially Implemented	Not Implemented	No Longer Applicable
FPCD-79-79 8/31/79	We recommend that the Director, OPM, work with other agencies to				
	--develop definitive standards for reporting costs and determining the scope of investigations;		X		
	--reach agreements to use these standards;		X		
	--share resources when appropriate; and			X	
	--encourage the use of improvements made by other agencies.		X		
	Once standards have been established and improvements made, OPM, as part of its monitoring process, should use the reported costs and other operational data to determine the most effective program, including assessing the potential savings that could result from consolidation. This would include identifying				
	--which agencies will conduct or assist in personnel investigations;		X		
	--an estimate of the workload which could be transferred, the number of staff years to make investigations, and the cost of these investigations; and			X	
	--potential benefits which would result from consolidation.		X		
	We also repeat our previous recommendation that the Congress consolidate into one law the authority to investigate and judge the suitability of Federal employees, including the potential of employees in sensitive positions to impair national security. (See p. 1)			X	

Report Number & Date	Recommendation	Implemented	Status as of February 1985 Partially Implemented	Not Implemented	No Longer Applicable
GGD-81-105 9/15/81	We recommend that the Secretary of Defense reprogram the 1982 budget to provide the Defense Investigative Service authority to hire the additional personnel needed to expedite the investigation and processing of personnel security clearances.	X			
	We recommend that the Attorney General request, and that the Director, Office of Management and Budget, approve authority for the FBI to increase the number of personnel in the Identification Division.		X		
	We further recommend that the Attorney General expedite implementation of the proposed automation program in that division.			X	
GAO/GGD 83-66 5/18/83	We recommend that the Secretary of the Navy establish a central adjudication facility for civilian and military personnel, in accordance with the requirement of DOD Regulation 5200.2-R, "Personnel Security Program."			X	

Government and Contractor Employees
With Security Clearances and SCI Access
As of December 31, 1983

Department/Agency	Total No. of Gov't Employees	Number of Government Employees with Clearances Top Secret	Secret	Confidential	SCI Access[1]	Number of Contractor Employees with Clearances Top Secret	Secret	Confidential	SCI Access
Defense	3,317,086	480,360	2,066,645	28,160	111,167	111,000	900,000	304,800	10,808
Postal Service	675,000	5	100	0	5	0	0	0	0
Veterans Administration	239,355	201	1,525	0	0	0	0	0	0
Health & Human Services	144,576	941	318	279	0	0	0	0	0
Treasury	124,287	6,871	2,995	274	1,755	185	0	0	2
Agriculture	120,000	750	1,500	2,900	155	0	0	0	0
Transportation	99,750	530	15,000	266	55	0	0	0	0
Interior	74,482	596	1,658	164	229	0	5	0	0
Justice	60,490	25,406	4,905	791	5,220	28	9	80	10
Tennessee Valley Authority	36,229	55	455	137	0	0	0	2	0
Commerce	35,104	1,285	7,150	100	215	0	25	0	0
General Services Administration	30,252	1,800	4,100	200	200	0	0	0	0
State	24,016	15,938	755	0	4,350	0	0	0	200
National Aeronautics & Space Administration	22,000	525	15,706	719	280	0	0	0	29
Labor	19,484	100	175	0	18	0	0	0	0

	Total No. of Gov't Employees	Number of Government Employees with Clearances				Number of Contractor Employees with Clearances			
		Top Secret	Secret	Confidential	SCI Access[1]	Top Secret	Secret	Confidential	SCI Access
Energy[2]	17,057	10,885	1,832	0	260	164,634	21,038	0	330
Housing & Urban Development	12,648	117	202	0	0	0	0	0	0
Environmental Protection Agency	11,368	54	853	79	14	15	18	3	7
United States Information Agency	8,200	3,162	852	0	71	0	0	0	0
Office of Personnel Management	6,827	40	405	0	25	1	0	0	0
Agency for International Development	5,232	1,075	1,925	0	100	0	72	50	0
Education	5,230	82	53	20	0	0	0	0	0
Small Business Administration	5,020	53	1,599	24	0	0	0	0	0
Others (24 with under 3,800 employees)[3]	21,967	4,326	5,808	105	301	728	4,440	0	2
TOTALS	5,115,660	553,935	2,137,142	34,156	122,396	276,589	925,605	304,935	11,388

NOTES: [1] Employees with sensitive compartmented information (SCI) access are required to have a top secret clearance. Therefore, the number of such individuals is included in the number of individuals with top secret clearances.

[2] The Department of Energy uses "Q" and "L" clearances which are comparable to the top secret and secret clearances used by other agencies.

[3] Information was not requested from the Central Intelligence Agency and National Security Agency. Furthermore, the following offices never responded to the April 1984 questionnaire requesting the data:

Executive Office of the President
Office of Management and Budget
United States Arms Control and Disarmament Agency
United States Trade Representative.

Executive Order 10450

Security Requirements For Government Employment

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U. S. C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U. S. C. 632, et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U. S. C. 118 j); and the act of August 26, 1950, 64 Stat. 476 (5 U. S. C. 22-1, et seq.), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

SECTION 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.

SEC. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

SEC. 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Civil Service Commission may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: *Provided*, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further*, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field preappointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

SEC. 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall readjudicate, or cause to be readjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

SEC. 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, readjudicate, or cause to be readjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

SEC. 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

SEC. 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: *Provided*, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Civil Service Commission that such person is eligible for such employment.

SEC. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

(iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.[1]

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Knowing membership →with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising← their rights under the Constitution or laws of the United States or of any State, or which seeks to overthrow the government of the United States or any State or subdivision thereof by unlawful means.[2]

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct.[3]

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Civil Service Commission, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Commission. The Commission shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Civil Service Commission, and other departments and agencies may use such facilities under agreement with the Commission.

---

[1] As amended by Executive Order 10548 of August 2, 1954.

[2] As amended by Executive Order →11785 of June 4, 1974.

[3] As amended by Executive Order 10491 of October 13, 1953.←

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (8)[4] of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

Sec. 9. (a) There shall be established and maintained in the Civil Service Commission a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Commission under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Civil Service Commission information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

Sec. 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

Sec. 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Civil Service Commission on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion, and the determination of the board shall be forwarded to the head of the department or agency concerned: *Provided*, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Civil Service Commission on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

---

[4] As amended by Executive Order 10531 of May 27, 1954.

Sec. 12. Executive Order No. 9835 of March 21, 1947, as amended,[8] is hereby revoked.

Sec. 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

Sec. 14. (a) The Civil Service Commission, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

(1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken the national security.

(2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Civil Service Commission shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance.[9]

(b) All departments and agencies of the Government are directed to cooperate with the Civil Service Commission to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

(c) To assist the Civil Service Commission in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this order, advise the Commission as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Civil Service Commission is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection.[9]

Sec. 15. This order shall become effective thirty days after the date hereof.

Dwight D. Eisenhower

The White House,
April 27, 1953.

---

[8] As amended by Executive Order →11785 of June 4' 1974, which revoked Executive Order 11605 of July 2' 1971.←

[9] As amended by Executive Order 10550 of August 5, 1954.

EXECUTIVE ORDER 10865

SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosures of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that those provisions and procedures recognize the interests of individuals affected thereby and provide maximum possible safeguards to protect such interest:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the armed forces of the United States, it is hereby ordered as follows:

SECTION 1. (a) The Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, and the Administrator of the Federal Aviation Agency, respectively, shall, by regulation, prescribe such specific requirements, restrictions, and other safeguards as they consider necessary to protect (1) releases of classified information to or within United States industry that relate to bidding on, or the negotiation, award, performance, or termination of, contracts with their respective agencies, and (2) other releases of classified information to or within industry that such agencies have responsibility for safeguarding. So far as possible, regulations prescribed by them under this order shall be uniform and provide for full cooperation among the agencies concerned.

(b) Under agreement between the Department of Defense and any other department or agency of the United States, including, but not limited to, those referred to in subsection (c) of this section, regulations prescribed by the Secretary of Defense under subsection (a) of this section may be extended to apply to protect releases (1) of classified information to or within United States industry that relate to bidding on, or the negotiation, award, performance, or termination of, contracts with such other department or agency, and (2) other releases of classified information to or within industry which such other department or agency has responsibility for safeguarding.

(c) When used in this order, the term "head of a department" means the Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, the Administrator of the Federal Aviation Agency, and, in sections 4 and 8, includes the Attorney General. The term "department" means the Department of State, the Department of Defense, and the Atomic Energy Commission, the National Aeronautics and Space Administration, the Federal Aviation Agency, and, in sections 4 and 8, includes the Department of Justice.

SECTION 2. An authorization for access to classified information may be granted by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an "applicant", for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.

SECTION 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of the reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the department concerned, an opportunity to appear personally before the head of the department concerned or his designee, including, but not limited to, those officials named in section 8 of this order, for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

SECTION 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.

(2) The head of the department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the department to be good and sufficient.

(b) Whenever procedures under paragraphs (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

SECTION 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the department concerned by an investigative agency pursuant to its responsibilities in connection with assisting the head of the department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered. In such instances a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

SECTION 6. Because existing law does not authorize the Department of State, the Department of Defense, or the National Aeronautics and Space Administration to subpoena witnesses, the Secretary of State, the Secretary of Defense, or the Administrator of the National Aeronautics and Space Administration, or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary or the Administrator, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination.

SECTION 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

SECTION 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a department by this order may be delegated to the

(1) Under Secretary of State or a Deputy Under Secretary of State, in the case of authority vested in the Secretary of State;

(2) Deputy Secretary of Defense or an Assistant Secretary of Defense, in the case of authority vested in the Secretary of Defense;

(3) General Manager of the Atomic Energy Commission, in the case of authority vested in the Commissioners of the Atomic Energy Commission;

(4) Deputy Administrator of the National Aeronautics and Space Administration, in the case of authority vested in the Administrator of the National Aeronautics and Space Administration;

(5) Deputy Administrator of the Federal Aviation Agency, in the case of authority vested in the Administrator of the Federal Aviation Agency; or

(6) Deputy Attorney General or an Assistant Attorney General, in the case of authority vested in the Attorney General.

SECTION 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

DWIGHT D. EISENHOWER

THE WHITE HOUSE
February 20, 1960

EXECUTIVE ORDER 10909

AMENDMENT OF EXECUTIVE ORDER NO. 10865, SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

By virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States, and as Commander in Chief of the armed forces of the United States, Executive Order No. 10865 of February 20, 1960 (25 F.R. 1583), is hereby amended as follows:

Section 1. Section 1(c) is amended to read as follows:

"(c) When used in this order, the term 'head of a department' means the Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, the Administrator of the Federal Aviation Agency, the head of any other department or agency of the United States with which the Department of Defense makes an agreement under subsection (b) of this section, and in sections 4 and 8, includes the Attorney General. The term 'department' means the Department of State, the Department of Defense, the Atomic Energy Commission, the National Aeronautics and Space Administration, the Federal Aviation Agency, any other department or agency of the United States with which the Department of Defense makes an agreement under subsection (b) of this section, and, in sections 4 and 8, includes the Department of Justice."

Section 2. Section 6 is amended to read as follows:

"Sec. 6. The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Administrator of the Federal Aviation Agency, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section 1(b), or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, and the proceeding involves the activity in connection with which the witness is employed, travel expenses and per diem are authorized as provided by the Standardized Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees of the executive branch of the Government or members of the armed forces of the United States not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An officer or employee of the executive branch of the Government or a member of the armed forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other department or agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination."

Sec. 3. Section 8 is amended by striking out the word "or" at the end of clause (5), by striking out the period at the end of clause (6) and inserting "; or" in place thereof, and by adding the following new clause at the end thereof:

"(7) the deputy of that department, or the principal assistant to the head of that department, as the case may be, in the case of authority vested in the head of a department or agency of the United States with which the Department of Defense makes an agreement under section 1(b)."

DWIGHT D. EISENHOWER

THE WHITE HOUSE

January 17, 1961

Glossary of Terms and Acronyms

Adjudication - The determination, based on specific criteria and past behavior, of the probability of a person's future behavior having an adverse affect on national security.

BI - Background Investigation - Includes all the elements of a NACI plus a credit check and personal interviews with selected sources covering specific areas of subject's background up to the past 7 years but not less than 5 years.

C - CONFIDENTIAL - The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security.

CS - Critical Sensitive - A position designation based on the assessment that an individual, by virtue of occupancy of the position, could cause "exceptionally grave damage" to the national security.

DIS - Defense Investigative Service - DOD component responsible for, among other things, conducting personnel security investigations for DOD military, civilian and contractor personnel.

DISCO - Defense Industrial Security Clearance Office - The office responsible for initiating investigations, issuing clearances and maintaining clearance records for DOD contractor personnel.

E.O. 10450 - Executive Order 10450 (Security Requirements for Government Employment) is the basic authority for the Federal Civilian Personnel Security Program. It requires that investigations be conducted on all persons entering the Federal civilian service, and makes agency heads responsible for maintaining within their agencies an effective personnel security program to insure that the employment and continued employment of each civilian in their agencies is clearly consistent with the interests of national security.

E.O. 10865 - Executive Order 10865 (Safeguarding Classified Information Within Industry) is the authority for agency heads to grant access to contractor personnel, for a specific classification category, only upon finding that it is clearly consistent with national interests to do so.

NAC - National Agency Check - Consists of record searches of selected agencies for information bearing on the loyalty, trustworthiness and suitability of individuals under investigation. A NAC may include checks of records at any or all of the following: Defense Central Index of Investigations; Federal Bureau of Investigation (both name and fingerprint checks); Office of Personnel Management, Immigration and Naturalization Service; and the State Department.

NACI - National Agency Check and Inquiries - Consists of a NAC plus written inquiries covering specific areas of the subject's background during the past 5 years.

NCS - Noncritical Sensitive - A position designation based on the assessment that an individual, by virtue of occupancy of the position, could cause "serious damage" to the national security.

OPM - Office of Personnel Management, formerly the Civil Service Commission.

PR - Periodic Reinvestigation - Consists of at least an updated Personal Information Questionnaire and a review of related personnel and security files. In addition, a NAC, subject interview, record searches, credit search, and resolution of issues raised since the last background investigation is ordinarily warranted.

PSI - Personnel Security Investigation - Any investigation required for the purpose of determining an individuals eligibility for access to classified information.

S - SECRET - The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

SAP - Special Access Program - Any program imposing "need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET or TOP SECRET information.

SBI - Special Background Investigation - Consists of the same components as a BI, however, the period of investigation is the past 15 years or to the subject's 18th birthday, whichever is shorter.

SCI - Sensitive Compartmented Information - Includes all information and material that require special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

SS - Special Sensitive - A position designation based on the assessment that an individual, by virtue of occupancy of the position, could cause "inestimable damage" to the national security.

TS - TOP SECRET - The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

5/3

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * *

BILL W. THURMAN
Deputy Director
National Security & International Affairs Division
GENERAL ACCOUNTING OFFICE

Q. On page 9 of your testimony you mention the need for investigators and adjudicators to get better training. Specifically, what dc you have in mind?

> If we are going to have consistent standards for investigations and adjudications, then we need to be sure that those individuals, involved with each process, understand, and know how to effectively implement the standards. From the government's point of view, we need consistency in protecting the information and consistency in the treatment of those individuals who are being considered for access. There can be more than one school but the curricula should be similar.

Q. On page 3 of your prepared statement you talk about "need to know" being the basic criteria for access. Is there any way for the government to ensure that the "need to know" principle is enforced?

> There is no way to provide 100 percent assurance of enforcement. However, periodic security inspections that check for compliance, and continual emphasis of this principal with those individuals who have security clearances are two ways to minimizing non-compliance.

Q. On page 11, you talk about the Office of the Secretary of Defense being responsible for personnel security policy throughout DOD. Practically speaking, can the policy group require the various military services and other components of DOD to follow established policy?

> From a practical point of view, the policy group does not have that authority. However, most policy matters are coordinated with various DOD components before they become formal policy. Sometimes, such policies have legally refined loopholes. If an impasse does occur between the policy group and a military service, for example, the issue can be submitted to the Deputy Secretary or Secretary of Defense for resolution.

Q. During your testimony, you mentioned the need to legislate the provisions of E. O. 10450, and gave as an example the cooperation that could be required of local law enforcement officials. Can you think of any other reasons?

> It has been suggested that such legislation, properly written, could be used to more effectively prosecute government and contractor personnel who compromise national security information.

Q. Is the 5-year reinvestigation period based on some demonstrated happening that indicates that 5 years is an appropriate length of time, or is it an arbitrary time frame based on workload? What is the optimum time period for reinvestigations?

> The 5-year period has been in use for a long time, but we do not know its origin. We have not studied the issue, however, it would be interesting to see how many clearance revocations are the result of period reinvestigations and how many are the result of notorious behavior of individuals where a periodic reinvestigation is not involved.

Q. You said the Defense contractors are required to formally report any adverse information concerning their cleared employees, but that there is no similar requirements for government employees -- in DOD or elsewhere. Such reporting, even if required for all government employees, appears to be a reactive response. Should not the government be more proactive in this area? In chronological order, what are the basic reasons for the revocation of clearances?

> The reporting of adverse information is a reactive response, but we believe that there are serious limitations as to what proactive measures could be employed and where their use would be beneficial. Consequently, we believe that the government should study the proactive approach. For the most part, statistics on denials of clearances and revocations -- when a distinction is made -- are not readily available. To our knowledge, DOD does not have a formal reporting process for this type of activity. It seems that the major DOD components do an analysis on a periodic basis. The Defense Industrial Security Clearance Office, which handles contractor employee clearances, gave us some information that may be useful. During the 4-month period ending January 31, 1985, the Clearance Office proposed denying or revoking almost 500 clearances. The basis for the proposed actions were as follows -- 36 percent for marijuana and hard drug use; 25 percent for alcohol abuse; 9 percent for sexual perversion, 7 percent each for financial problems mental illness, and criminal conduct; and 9 percent for all other reasons.

Chairman ROTH. I would now like to call forward Brigadier General Charles Scanlon, Deputy Chief, Intelligence Command, Department of the Army.

Senator NUNN. Mr. Chairman, on the last witness, we have certain questions for the record. If we could get them to answer, we will submit them for the record.

Chairman ROTH. Without objection, so ordered.

Please raise your right hand. Do you swear the testimony you give before the subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

General SCANLON. I do.

Chairman ROTH. Thank you, General. Please be seated and proceed with your statement.

Senator NUNN. Mr. Chairman, General Scanlon has a longer statement which I suggest we put in the record, and I think he is prepared to summarize his statement. I believe he plans to show a brief film, and then he will really, in effect, be introducing our next witness. At that stage, after we get through with General Scanlon's testimony, it is my suggestion, Mr. Chairman, that we have a clearing of the room because there is a need to protect the next witness' identity and face and turning away of all cameras at the stage after he finishes his testimony.

Chairman ROTH. That will be the procedure. Your full statement will be included in the record.

TESTIMONY OF BRIG. GEN. CHARLES F. SCANLON, DEPUTY COMMANDER, INTELLIGENCE COMMAND, DEPARTMENT OF THE ARMY

General SCANLON. Thank you, sir. Mr. Chairman, members of the committee, as was indicated, I'm the Deputy Commander of the U.S. Army Intelligence and Security Command. I welcome the opportunity to present the subversion and espionage directed against the U.S. Army program, a program which provides an awareness of methods used by foreign intelligence services and other disruptive elements to obtain information from or to enlist the services of Department of Army personnel.

The short title for this program is SAEDA and it focuses on the Army's efforts to protect its military and civilian personnel against situations that can adversely impact on the security of the United States. A positive aspect of our program is the requirement that all major Army Commands establish a SAEDA training program.

Under the program, all Army personnel from the national level down to the tactical troop unit receive an annual SAEDA briefing to reinforce this program.

The Army Intelligence and Security Command is tasked by Army regulation to prepare and present SAEDA briefings at echelons above corps level. Tactical units at corps and below levels receive direct assistance from the counterintelligence personnel assigned to the supporting tactical military intelligence unit.

In the absence of Intelligence and Security Command or tactical intelligence personnel, SAEDA briefings will be presented by unit security officers or managers. These briefings take the form of oral presentations or filmed features prepared by the intelligence community and tailored for a particular audience or geographic area.

To illustrate, I would like to present extracts from a film produced for and used in the Army's SAEDA program at the Pentagon. This film clip, narrated by an INSCOM counterintelligence agent, will show methods and techniques used by our adversaries to obtain national security information. It will highlight reasons why people sometime fail to report approaches and incidents that may lead to the degradation of our personnel and systems security programs; it will specify reporting procedures to follow if and when an individual feels that he or she has been approached by a hostile intelligence agency. Further, it will cite the specific regulations of the military services governing and authorizing their respective participation in the subversion and espionage program.

[At this point in the hearing, there was a showing of a video film. At this point in the hearing, Senators Cohen and Gore entered the hearing room.]

General SCANLON. Over the past few years within the Army, we have seen an increase in the number of SAEDA incidents reported, investigated and exploited. I want to just show you three brief charts that indicate some kinds of trends that we are seeing.

Mr. Chairman, if you can see that chart, what that indicates is that from fiscal year 1982 until fiscal year 1984, in terms of total number of incidents, we see an increase from 369 to 481. I have also shown a breakdown where around the world those are taking place. The red indicates 259 incidents in the United States; the green line indicates 156 in Europe and 41 by the blue line taking place in the Pacific. The next chart, please.

In a look at our current incident investigative effort in fiscal year 1985, first quarter, we see a total of 124 incidents taking place, 72 of those in the Continental United States; 37 in Europe and 15 in the Pacific. Finally, on our last chart, our investigation and what that is telling us is we think that our SAEDA program within the Army is working well for us. Seventy percent of the counter-intelligence we are receiving originates from a SAEDA source or someone who thinks they may have been contacted by a hostile intelligence service.

Since 1978, we have seen a 400-percent increase in reporting of incidents, indicating both a rise in the number of incidents taking place and security awareness. Ninety-four of these SAEDA incidents in fiscal year 1984 were referred for possible offensive exploitation where we could then learn something about the hostile services and turn their operations against them.

In our 1984 fiscal year efforts, our results were that operatives from six hostile intelligence services were positively identified as operating against the U.S. Army.

Investigation and/or exploitation of reported incidents requires close coordination and continuous exchange of information between U.S. national agencies, the FBI, CIA and the military service investigative agencies. Total investigative efforts that we expend to curtail the threat from our adversaries is bonded to a common link. That vital link in the SAEDA program is the individual; the individual soldier, non-commissioned officer, officer or civilian.

Mr. Chairman, as has been stated, I have prepared a written statement for you detailing a real world example of the continued pervasive intelligence threat to the United States Army posed by the hostile intelligence services and highlighted in the Otto Gilbert case.

I would like to take a moment and summarize the Otto Gilbert case because it demonstrates how the SAEDA program works, from the time it is reported through exploitation.

In December 1977, Chief Warrant Officer Jamos Szmolka, a United States Army member stationed in West Germany while visiting his mother and family in Budapest, Hungary, was approached by representatives of the Hungarian Intelligence Service. Szmolka was taken to a meeting with the Hungarian Government official by a family friend. This official made it abundantly clear that he was a Hungarian intelligence officer and he wanted NATO and U.S. military information in exchange for favorable treatment of Szmolka's mother and family, then residing in Hungary.

Szmolka immediately reported this recruitment approach to U.S. Army Intelligence authorities upon his return to West Germany and agreed to cooperate to exploit this threat by Hungarian intelligence.

Under U.S. direction, Szmolka told Hungarian Intelligence that he would cooperate. As a result, he was told his mother would be allowed to visit him in West Germany. He was asked to collect information concerning the U.S. Army and was told he could make tens of thousands of dollars.

Szmolka maintained letter and telephonic contact with the Hungarian Intelligence Service and in December 1979 he attended a personal meeting in a third country in Europe, just prior to his return to the United States.

At a series of meetings with Hungarian Intelligence Service representatives, Szmolka was asked to collect other NATO and U.S. war plans, nuclear capabilities, storage sites and information concerning the deployment of Pershing missiles to Western Europe. Szmolka was promised $20,000 if he was able to provide a U.S. Army cryptographic machine.

Szmolka was provided two addresses to write to in Budapest and instructed to write monthly. He was told that the Hungarian Intelligence Service would meet him in the United States.

As the European phase came to a conclusion, Army Intelligence had been able to determine the Hungarian Intelligence Service's methods of operations, procedures, personalities, interests, communication channels and other related counterintelligence information.

The level of espionage started at low level, but quickly elevated to strategic collection. From January 1980 to March 1981, Szmolka maintained letter contact via codes. In March 1981, Szmolka traveled again to Europe to meet with representatives of the Hungarian Intelligence to receive requests against the U.S. Army Signal School and against U.S. nuclear capabilities in the United States.

Communications between Szmolka and Hungarian Intelligence was revised and he was provided a new mailing address in yet another country in Europe. Additionally, he was provided two meeting locations in the United States. One in Atlanta, GA, and the other in Augusta, GA, where he was stationed. These meeting locations would be used in the event that Szmolka was able to obtain secret or top secret information.

Szmolka maintained correspondence with the Hungarian Intelligence Service and alerted them when he was able to collect the desired information. Hungarian Intelligence initiated arrangements to meet Szmolka in Augusta, GA, in the spring of 1982. April 15, 1982, Szmolka received a telephone call at his residence from an individual later identified as Otto A. Gilbert, using a pre-arranged code. Gilbert confirmed he was, in fact, the Hungarian Intelligence representative, and on April, 17 Szmolka met Gilbert under the observation of U.S. counterintelligence authorities and at a precipitous moment, FBI special agents moved in and arrested Gilbert.

Gilbert, faced with the possibility of two life sentences, entered into plea bargaining with the U.S. Justice Department in exchange for a 15-year sentence, but his arrest and subsequent cooperation provided significant counterintelligence information to the U.S. authorities and U.S. Army.

I would like to now, sir, if I may, move to a second example of an SAEDA incident and subsequent exploitation of an individual currently on active duty but beginning in another part of the world. Because he is currently on active duty, I ask his name not be passed to the public.

Chairman ROTH. So ordered.

[General Scanlon's prepared statement, with attachments, and responses to written questions follow:]

PREPARED STATEMENT OF BRIG. GEN. CHARLES F. SCANLON

Mr. Chairman, Members of the Committee, I welcome this opportunity to present a specific example of the continuing and pervasive intelligence threat to the United States Army posed by hostile intelligence services. The methods used against our personnel by foreign services underscore the need for vigilant personnel security and intensive security awareness programs. Your past and continuing support for such programs is essential to maintaining and improving Army security.

Introduction

The Otto Gilbert Case

In what has become known as "The Otto Gilbert Case," the methods used against our personnel by hostile services--in this case Hungarian intelligence--are vividly demonstrated. A review of this case, which culminated in the arrest of United States citizen Otto Gilbert on 17 April 1982 in Augusta, Georgia, provides a wealth of information concerning how the Hungarians attempt to identify, target, recruit and direct United States Army members in espionage activities.

It is important to note that the Army member involved in this case acted under the direction of United States counterintelligence authorities. The overseas phase was coordinated with the CIA and the US phase was conducted under the control of the FBI. My testimony will concentrate on hostile methods and procedures directed at the United States Army.

Background

The Approach in Hungary

In December 1977, Chief Warrant Officer Jamos Szmolka, a United States Army member stationed in Mainz, West Germany, traveled on authorized leave to Budapest, Hungary, to visit his mother. This was Szmolka's third visit to Hungary and Szmolka had no reason to expect this trip would be more eventful than his previous trips. It would be, however, as Hungarian intelligence was waiting for him. Probably because of his repeated travel to Hungary, he had come to the attention of Hungarian authorities, and through subsequent checking, enough factors existed for the Hungarians to believe that Szmolka might be recruitable as an espionage agent.

Szmolka was born in Hungary but had fled the country in 1956 during the uprising. Eventually resettled in the United States, Szmolka became a naturalized United States citizen and a career Army member. Though married (to another United States Army member), Szmolka's closest blood relatives were his now aged mother and married sister, both of whom were citizens and residents of Hungary.

The first approach to Szmolka by Hungarian intelligence was both blatant and direct. While at his mother's home, a family friend who worked for the Hungarian government took Szmolka aside and told him that a "representative of the government" wished to speak with him, privately, away from his mother's home. Apprehensive but curious, and concerned that he do nothing to cause trouble for his relatives, Szmolka agreed to the meeting. The meeting took place at a restaurant where Szmolka was introduced to Lajos Perlaki, a Hungarian intelligence officer. After only minimal amenities and general conversation exchanges, during which Perlaki made it clear he was familiar with Szmolka's background and family, the intelligence "pitch" was made. The overture was blunt. In exchange for favorable treatment for

Szmolka's family, the Hungarian government desired NATO and US Forces military information.

As he traveled back to West Germany from Hungary in January 1978, Szmolka agonized over what to do. He knew that he was required by Army security regulations to report the approach but to do so could jeopardize his family. He might never see them again. To cooperate with the Hungarians in espionage was unthinkable, but the implications of unfavorable actions against his family was stark and easily imagined. Perhaps he should simply sever all ties with his relatives in Hungary and never return to Hungary again. Each course of action was fraught with unpleasant and unforeseeable consequences. Szmolka made the right decision. Upon his return, he reported the Hungarian intelligence approach to United States Army authorities.

The hostile intelligence methods used by the Hungarians in this espionage approach to Szmolka are both classic and effective. The approach was made by the foreign service in the foreign country where their control of the situation was absolute. Their assessment of the importance to Szmolka of his family ties, as evidenced by his recurring visits to Hungary to visit his old and ill mother, was essentially correct. By combining the promise of favorable treatment with the implied threat of unfavorable treatment both to him and his family if he did not cooperate, Hungarian intelligence had set a powerful trap. This hostile methodology is used again and again, with variations depending on the targeted soldier, against our personnel with relatives in hostile countries.

Significant Developments

The Europe Phase

In June 1978, Szmolka returned to Hungary, thereby implicitly signifying his agreement to cooperate. At his sister's residence in Budapest, Szmolka received a letter directing him to contact Perlaki. At the subsequent meeting, again held in a restaurant, it was made clear to Szmolka by Perlaki that the Hungarian government considered Szmolka to be cooperative and as evidence of good faith, the Hungarian government had arranged to allow Szmolka's mother to visit Szmolka in the West. Szmolka was repeatedly offered money (approximately the equivalent of $1,500) and was told that in addition to favorable treatment for him and his relatives, "tens of thousands of dollars" were to be made by cooperating with Hungarian intelligence.

When told that Szmolka had not brought military information with him to Hungary, and that it had been fortunate he had not as he had been searched at the Hungarian border, Perlaki explained that during all future crossings Szmolka would be assisted by Hungarian authorities. Szmolka was then tasked to collect such innocuous military information as a copy of the Uniform Code of Military Justice, training manuals concerning use of the polygraph, procedures for military police and criminal investigations, and a copy of the standard operating procedures for Szmolka's office in the Criminal Investigation Detachment at Mainz, West Germany. Szmolka was to bring these and similar unclassified documents to Perlaki at future meetings. Though no formal recruitment agreement was signed, this meeting formalized Szmolka's ostensible recruitment by Hungarian intelligence.

On 24 June 1978, Szmolka and his wife left Budapest in his privately owned vehicle with Szmolka's mother, now allowed to visit in the West. Upon arrival at the Hungary-Austria border, Szmolka was directed to pull out of the line of vehicles awaiting processing and allowed across the border without problem or delay. At the small facility stop in "no man's land" between Hungary and Austria, a smiling Perlaki approached Szmolka and informed him that Hungarian intelligence had arranged his easy crossing and that all future crossings in and out of Hungary would be as easy.

At the end of her authorized visit, and unwitting of her son's involvement in intelligence activities, Szmolka's mother returned to Hungary on a commercial flight in August 1978.

From August 1978 until December 1979, Hungarian intelligence maintained frequent contact with Szmolka in West Germany both by mail and by telephone. Szmolka continued to act cooperative but professed inability to return to Hungary for personal meetings because of pressing military duties and also suggested that too frequent trips to Hungary could bring him to the attention of Western authorities. Eventually, as an alternative to Szmolka returning to Hungary, the Hungarians arranged a personal meeting to be held in another European country near the Hungarian border.

In December 1979, Szmolka traveled to the designated third country by train from West Germany to meet Perlaki. A second operative, Vince Konc, apparently Perlaki's superior, was also present. Though Konc and Perlaki were initially critical of Szmolka for not meeting with them earlier, they were appeased by Szmolka as he explained his reasoning and provided them with information they had requested. Convinced of Szmolka's sincerity and willingness to provide information, the effort immediately escalated.

In a series of three meetings held over two days in various public facilities, the Hungarian officers questioned Szmolka exhaustively about his past and present military assignments. The Hungarian officers claimed their intent was not to hurt the United States and that their only interests were in information concerning actions or weapons that might be employed against Hungary in the event of hostilities. In detailed questioning Szmolka was asked about his knowledge and tasked to collect information concerning NATO and US war plans, nuclear capabilities and storage sites, information concerning deployment of new Pershing missiles to Western

Europe, and information concerning cryptographic communications. Szmolka was specifically promised a minimum of $20,000 if he could obtain a US Army cryptographic machine. When Szmolka protested that he had little access to the type of material desired by Hungarian intelligence, he was told that his badge and credentials could afford him entree to areas which were restricted to others. Additionally, he was told to look for others to provide him information and these others could, thereby, establish lucrative financial sidelines.

As Szmolka became due for reassignment from West Germany to the United States, the Hungarian officers also used these meetings to establish communication channels with Szmolka after his departure from Europe. Szmolka was provided two mailing addresses in Budapest and instructed to write monthly to report to Hungarian intelligence. Szmolka was told that the Hungarians could meet him in the future in Mexico, Canada, or the Caribbean. Significantly, the Hungarians mentioned that they could even meet him within the United States should the information he collected be sufficiently valuable.

An interesting sidelight of the December 1979 meetings concerned Szmolka's mother. The Hungarians told Szmolka several times that they trusted him because he came from a good Hungarian family. Szmolka asked, if that were true, why his mother was treated so shabbily by the Hungarian government, forced to live a pauper's existence on a tiny government pension, diminished by the fact that she was not a Communist Party member. Szmolka was assured his mother would receive additional money in the future, channeled to appear the money came from Szmolka when in fact the increase would be arranged by Hungarian intelligence. The Hungarians kept this promise, continuing the monthly supplements for the duration of Szmolka's involvement.

As the Europe phase came to an end with the December 1979 reassignment of Szmolka from Europe to the United States, Hungarian intelligence methods, procedures, personalities, interest, communication channels and related counterintelligence information had been determined. The level of espionage tasking had escalated from very low unclassified US military information to strategic defense plans, weapons, and communication systems. From the original offer of simple government assistance in obtaining visas and facilitating border crossings, compensation and remuneration incentives had escalated to pension supplements and the possibilities of thousands of dollars for obtaining specific items. From personal meetings conducted within the denied area of Hungary itself, meeting arrangements had developed to third country locations with the possibility of meetings even within the United States. The building intensity and commitment by Hungarian intelligence to espionage efforts against the United States Army through Chief Warrant Officer Szmolka had become starkly clear.

Significant Developments

The United States Phase

From January 1980 to March 1981, Szmolka maintained contact with Hungarian intelligence from Fort Gordon, Georgia, by letters using brevity codes to the Budapest addresses. Szmolka consistently presented himself as willing to fulfill Hungarian espionage requirements but said he was hampered in his efforts by nonsensitive placement at Fort Gordon complicated by the slow and cumbersome method of communication arranged by the Hungarians. Szmolka requested meetings with the Hungarians, preferably in the United States or nearby countries, to discuss his problems and to arrange communication and reporting improvements, but the Hungarians were not prepared to meet with him as he requested. After a period of essentially stalemated exchanges, arrangements were finally agreed to for another meeting in Europe.

In March 1981, Szmolka flew from the United States to the capital of a western European country to meet his Hungarian handlers. Again he was met by both Konc and Perlaki, who were elated at this coming and went to great lengths to "wine and dine" Szmolka in showing appreciation of his efforts. In fact, Konc and Perlaki became so intoxicated at one session at a restaurant on the outskirts of the city that Szmolka had to drive the two back to the capital proper in the Hungarian Embassy car they were using. Nevertheless, the March 1981 meetings were very productive. As evidence of his efforts for the Hungarians in the United States, Szmolka provided several rolls of film containing information he had collected at Fort Gordon. The Hungarians questioned him extensively concerning his activities since they had last met in December 1979. In addition, he was queried about

Fort Gordon and his duties there, and the possibilities of his being able to acquire highly classified information. Of special interest to the Hungarians was the classified Army regulation concerning movement of nuclear weapons, and instruction materials at the US Army Signal School at Fort Gordon dealing with cryptographic systems. Szmolka was provided a new address through which to report his progress, in yet another western European country, that would allow improved security and quicker response. A detailed code of collection requirements was furnished for reporting and Szmolka was assured that a representative of Hungarian intelligence would service him in Georgia if he succeeded in obtaining the desired information.

Two sites in Georgia, one in Atlanta and one in Augusta, were selected as meeting locations should Szmolka need to be met and relieved of highly sensitive information. A contact code was arranged for mutual recognition between Szmolka and the representative sent to service him. Szmolka was paid $3,000 for his services and expenses and encouraged to exercise both resourcefulness and prudence upon his return to espionage activities at Fort Gordon.

Termination

The Arrest of Otto Gilbert

For approximately one year after the March 1981 meeting in Europe, Szmolka reported to the Hungarians by coded letters through the second country mailing address, claiming limited success at obtaining information according the list of requirements. In early 1982, in an effort to force the Hungarians to surface a representative to service Szmolka in Georgia, Szmolka reported he had obtained highly classified information and requested that he be met. On 27 March 1982, Szmolka received a letter from Hungarian intelligence informing him that he would be met in Augusta on 17 April by an individual who would pay him handsomely and relieve him of the material.

An arrest reception was arranged in Augusta for the Hungarian operative. On 15 April, Szmolka received a telephone call at his home late at night from an individual later identified as Otto Gilbert. Gilbert used the identifying code confirming himself as the representative of the Hungarians and reconfirmed the meeting arrangements for 12:00 noon, Saturday, 17 April at the Confederate Monument in downtown Augusta.

On 17 April 1982, Otto Attilla Gilbert, expatriate Hungarian and naturalized US citizen, contacted Szmolka at the Confederate Monument meeting site, under the observation and full surveillance of US counterintelligence authorities. Szmolka, equipped with an audio transmitter on his person, carried out the meeting with Gilbert, unquestionably establishing Gilbert's knowing involvement in espionage activities. At the conclusion of their meeting, Gilbert was arrested by agents of the Federal Bureau of Investigation as he exited Szmolka's vehicle in possession of classified US defense information.

In the weeks of interrogation that followed his arrest, Gilbert, faced with possible life imprisonment, entered into plea bargaining with the United States Justice Department, agreeing to cooperate fully with US authorities in exchange for 15 years imprisonment. Gilbert's arrest and subsequent cooperation provided significant counterintelligence information not only to US authorities but also to other friendly Western intelligence services.

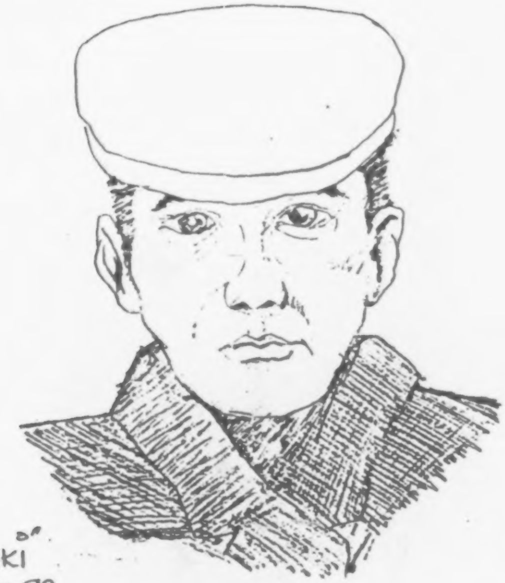
Summary

The Otto Gilbert Case is an example for the US Army's Subversion and Espionage Directed Against US Army (SAEDA) program, which provides US Army personnel with examples of hostile intelligence methods and requires immediate reporting of known or suspected overtures. This program has again and again proven extremely valuable in providing early recognition of hostile efforts and in affording US authorities opportunities to both limit damage and to exploit selected situations with aggressive counterintelligence procedures. The training and reporting requirements inherent in this program constitute our basic counterintelligence defenses.

Because of recurring experiences of our personnel being approached by hostile intelligence services while traveling through or visiting hostile countries, various programs requiring advance notification of travel are conducted to identify, in advance, those soldiers planning such travel. These programs serve several important security objectives, including specific warnings in advance to personnel at risk, providing an information base concerning unusually long or frequent travel to hostile countries, and allowing for follow-up security debriefings of travelers upon their return.

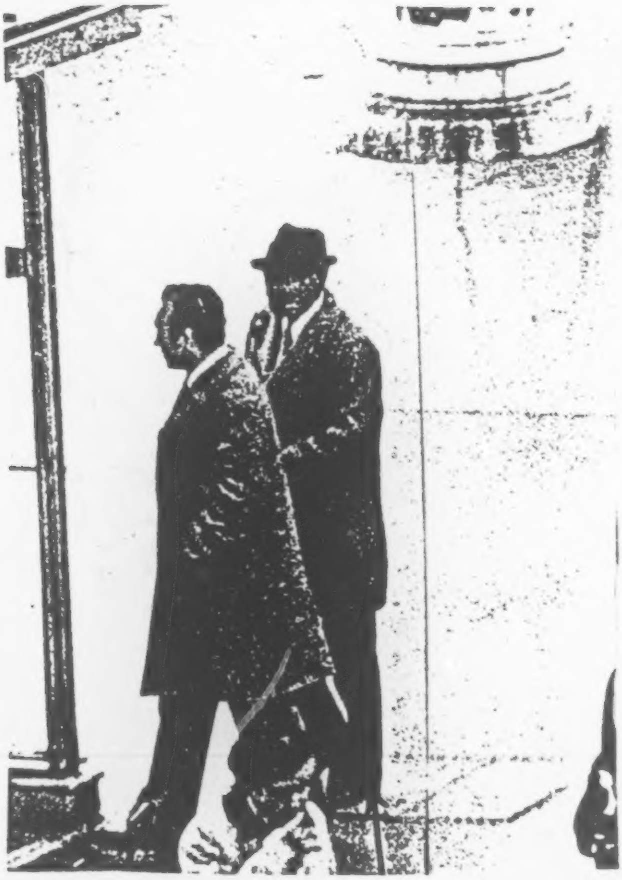
While the foreign espionage threat in this case was posed by the Hungarian service, the methods used are standard for Soviet and other Warsaw Pact services. Especially in Europe, where we maintain a large presence and because of the many ethnic ties and contacts of our personnel with Soviet and East European countries, the hostile intelligence threat is enormous and requires constant and aggressive security awareness training and personnel security programs.

The quality of our personnel security programs will always be dependent on the quality of our personnel and their awareness of the hostile foreign threat. The courage, common sense, loyalty, sense of duty and responsibility which Chief Warrant Officer Szmolka displayed reflects those personal and professional attributes which we seek in our soldiers. His efforts in behalf of the US Government in this counterintelligence activity far surpassed that which could be expected of the average citizen or soldier. It is interesting to note that both Szmolka and Gilbert were Hungarian by birth, and that both were naturalized United States citizens.



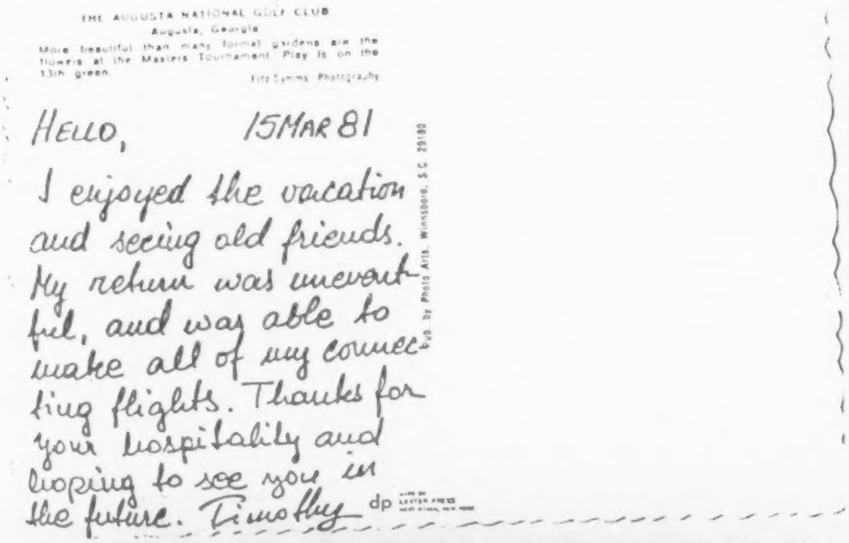
"PERLAKI"
8 DEC 79

Artist Rendition of Lajos Perlaki
8 December 1979



Hungarian officers Lajos Perlaki (left) and Vince Konc (right)
8 December 1979

Hungarian officer Vince Konc
8 December 1979



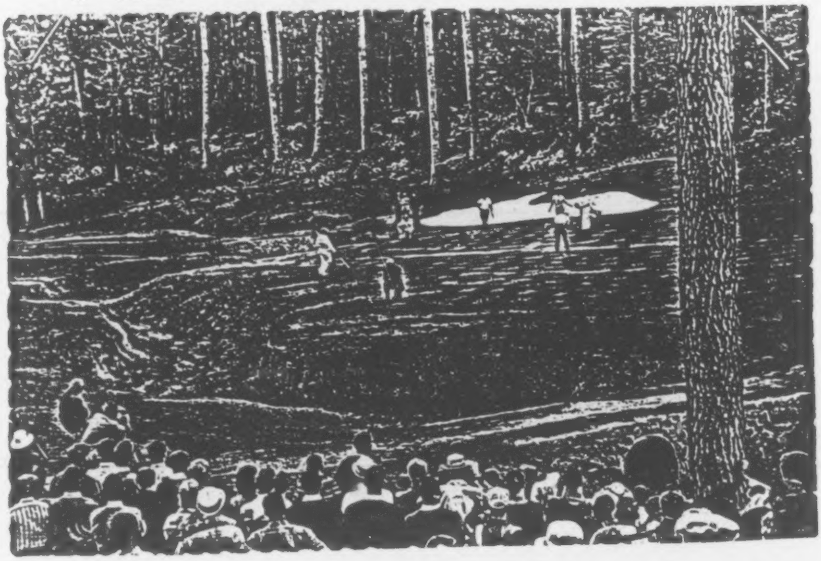
THE AUGUSTA NATIONAL GOLF CLUB
Augusta, Georgia
More beautiful than many formal gardens are the flowers at the Masters Tournament. Play is on the 13th green.
Fitz Symms Photography

Pub. by Photo Arts, Winnsboro, S.C. 29180

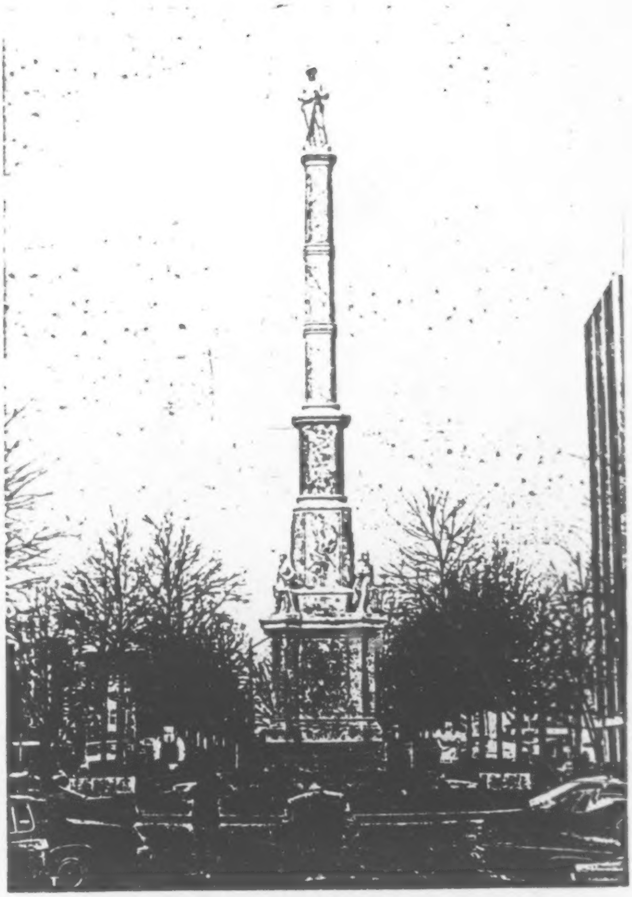
HELLO, 15MAR81

I enjoyed the vacation and seeing old friends. My return was uneventful, and was able to make all of my connecting flights. Thanks for your hospitality and hoping to see you in the future. Timothy

dp



Post card to Hungarian intelligence indicating
"safe arrival" of Szmolka at Fort Gordon, Georgia



The Confederate Monument contact site in Augusta, Georgia

US citizen and Hungarian intelligence operative Otto Atilla Gilbert
Arrested in Augusta, Georgia 17 April 1982

5/3

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * *

BRIGADIER GENERAL CHARLES F. SCANLON
Deputy Chief, Intelligence Command
DEPARTMENT OF THE ARMY

Q. Do you see a vulnerability with foreign nationals working at U. S. military installations, consulates, or U. S. contractor facilities abroad?

> Yes, there is some degree of vulnerability. Jobs that are offered to foreign nationals involve limited to comprehensive personnel screening processes for security reasons. These non-U. S. citizens overseas who require access to classified information undergo a comprehensive personnel security investigation. If there are periods of a subject's life that cannot be corroborated by normal investigative techniques, we are authorized to conduct a polygraph examination to prove or disprove what the individual has told us. If the investigation indicates the subject is a responsible person who reportedly exercises good judgement and is a person of acceptably high integrity, we grant what is called a Limited Access Authorization. This is not an unqualified security clearance, but is a closely defined authorization applicable to precisely identified documents and/or functional areas. Additionally, the foreign national is unlikely to owe any loyalty to the U. S. Any loyalty is most likely to have its base in financial considerations. Finally, the foreign national employee is more likely to have relatives in a Communist bloc area upon whom duress can be exercised.

Q. Is it true that the KGB and GRU place a higher priority on cultivating U. S. servicemen and other Americans overseas? Is it your experience that certain Americans are more susceptible to Soviet approaches overseas than they are at home?

> In response to the first question, the answer is...YES! This can be attributed to several factors: First, the sheer number of individuals under the control of the Soviet intelligence apparatus overseas; freedom of movement by intelligence operatives, as opposed to the travel

restrictions within the United States; and the psychological and cultural susceptibility of an American living in a foreign environment. Experience has shown that certain Americans are more susceptible to Soviet approaches overseas than they are at home. The desires of most Amerians to blend into and be accepted by foreign nationals, in their home country, contributes to that susceptibility. Anyone in a strange country desires some pleasure from speaking his own language, and often this opportunity is presented to complete strangers. Americans at home, among their friends and associates, experience more inhibitions against favorable response than they do when overseas, more or less along, and, temporarily at least, beyond the reach of U.S. law and the disapproval of their home folk. An American abroad, especially when he has had no intelligence or investigative experience, is likely to feel that his favorable response to an approach made in a foreign country is not as likely to be surfaced as it might be if the approach is made in the USA.

Q. In what social environment are Soviet agents most likely to approach American servicemen?

Drinking establishments and bars frequented by U. S. servicemen and women, during their off-duty time, are the most likely social environment used by Soviet agents to initiate contact. The social atmosphere within these establishments lends itself to the "casual" approach by a hostile intelligence agent. Technical conventions or meetings; in-country local language courses conducted by local residents; conferences sponsored by a host nation also present hostile intelligence services with favorable target environments. The Soviets use either an informal or formal approach to contact an individual of interest on a totally "innocent" basis.

Q. In the Szmolka case, Otto Gilbert was an "illegal," that is to say, he was not in the diplomatic service of his country but was instead a naturalized citizen of the United States working here as an agent of Hungarian intelligence. Is it common to find "illegals" engaged in this kind of work in this country? Or was the Szmolka case unique in that sense?

It is not common to find, that is, catch, illegals working in this country, but several have been surfaced over the years. The term "illegal," within the intelligence community, defines an individual who is dispatched, that is, sent to service agents in a "denied" area. Other "illegals" have more elaborate "legends," but they basically serve the same intelligence function. In that context, the Szmolka case is not unique.

Q. American servicemen are instructed to report approaches by hostile intelligence agents. Janos Szmolka did, as we have seen. Can you tell us your estimate of the percentage of servicemen who do report these kinds of contacts? Is more educational effort required to increase the number of reported contacts?

> To set a percentage, even an estimated figure, on the number of U. S. military personnel who do report their exposure to hostile contact would be in error. We can only hope that the percent level of reported incidents based on actual contact is on the high side of the percentile scale. One positive aspect we can point to with certainty is the correlation of reporting to SAEDA training. The more training provided, the more incident reports received. Since instituting our requirement for annual SAEDA training for Army personnel, our SAEDA incident reporting has increased significantly. The key to success is to keep security awareness fresh in the minds of our soldiers.

Q. How many espionage cases has Army Counterintelligence made during the past ten years?

> I would like to preface my response with a qualifying statement.... "The implication of the Army's counterintelligence involvement in espionage cases encompasses the following cycles: The investigative phase, the indictment, conviction, and incarceration phase." In this light, we have identified a total of 8 cases which fit all these parameters. Additionally, we have been involved in 16 other cases which have involved other forms of neutralization of the espionage effort but did not result in an indictment, conviction, or incarceration. Neutralization in these cases has taken the form of: Bans on reenlistment; non-judicial punishment; and/or loss of clearance/removal of individual by reassignment. All of these processes were the result of commander initiated action. Thus, there are a total of 24 cases where the Army has neutralized espionage activity in the past ten years.

Senator **Nunn**. Mr. Chairman, the next witness we will refer to as Sergeant Smith, and he affords a unique opportunity for us to view Soviet methods and procedures against our servicemen. We thank the Army for their cooperation in making this witness available. For over 10 years, Sergeant Smith worked as a double agent for our Government against the Soviets. Though the operation is over now, there are still major areas of sensitivity we wish to avoid in the testimony and questioning of Sergeant Smith.

Therefore, I have asked that Sergeant Smith's testimony concentrate on how the Soviets went about this espionage effort and address specifically those areas concerning specifically our U.S. countermeasure methods, and I would ask the questions that our colleagues pose concentrate on the Soviet methods and not our methods.

We will also preserve his anonymity with the use of a screen and assumed name since we understand his utility in the U.S. intelligence community will continue.

This operation was started, maintained successfully over a decade and ended for operational reasons beyond the scope of Sergeant Smith's testimony here today. If any of the members have questions in these areas, we can discuss those with Sergeant Smith in closed session, but I am confident Sergeant Smith's testimony in open session concerning how the Soviets dealt with him will give us all a better understanding of how the KGB works and the threat it represents to servicemen around the world, regardless of rank, position, or background.

Again, I would request the subcommittee members address their questions to those areas of Soviet methods and procedures.

Chairman **Roth**. As has been indicated, due to his continuing use in sensitive activities for the U.S. Army, our next witness will testify while sitting behind an opaque screen. All cameras will have to be relocated so as to show photography only from the audience side of the screen. It will be necessary to clear the room prior to bringing the witness in.

Prior to doing so, I request that all cameras be relocated away from the area in front of the screen where the witness will be seated. Once that is done, I will ask that the room be cleared so that the witness may be brought in.

So at this time, if the cameras would go to the rear of the room.

Senator **Nunn**. Mr. Chairman, we may be able to accommodate the cameras. If I could suggest we turn the cameras down or away toward the back of the room in the interim here. Let's see how large the screen is and then when we come back, we will see how many cameras there are. We may have to push them back that way.

Chairman **Roth**. I would then ask the rest of the room to be cleared.

[Brief recess. Senators present at the time of the recess: Senators Roth, Cohen, Nunn, and Gore. Senators present at the reconvening of the hearing: Senators Roth, Cohen, Nunn, and Gore.]

Chairman **Roth**. Will you raise your right hand? Do you swear the testimony you will give before the subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Sergeant **Smith**. I do.

Chairman ROTH. The subcommittee will be in order.

Sergeant Smith has been sworn in, so at this stage, we would ask you to proceed with your testimony. Sergeant Smith.

TESTIMONY OF SERGEANT "SMITH," U.S. ARMY

Sergeant SMITH. Thank you, sir. I am a United States Army Sergeant with 15 years military service. For more than 10 of those years, the Soviet Union considered me an agent of the KGB, and I was met by their intelligence officers on four different continents in places as far away and exotic as Bangkok, Thailand, and as close to home as New York City.

Unknown to the Soviets, I was working for U.S. counterintelligence. An overview of my activities as a source for the KGB will, I am confident, demonstrate how pervasive, unrelenting and skilled the Soviet intelligence agencies are in pursuit of American military and Government personnel to serve Soviet purposes.

That this threat is real and knows no boundaries is very clear to me. As a native-born American in military service without apparent exploitable circumstances, I was a Soviet target. Quite literally, it could happen to anyone.

It all began with a game of chess at a bar in Bangkok. There, in the early 1970's, I met a number of foreigners at a chess club I occasionally frequented during off-duty time. I also played chess in a bar owned by a Swiss citizen, the principal patrons of which were Europeans. It was at this bar possibly on the recommendation of someone from the chess club that a man I came to know as "Tori" approached me. I did not know it at the time, but later learned that Tori was a Soviet diplomat assigned to the Russian Embassy in Bangkok. We talked about chess; we introduced ourselves and simply shot the breeze in a pleasant, otherwise nondescript manner.

Tori then suggested that we meet sometime for a chess game in a quieter environment. I agreed, and we arranged to get together in a coffee shop a few days later. Our coffee house get-together produced no chess. Instead, Tori supplied the beer and asked apparently innocuous questions about where I worked, marital status, and so on.

Tori continued his personal development of me for some months, all asking seemingly innocent questions, getting to know and understanding. Tori wanted me to get to know, accept and trust him. We moved from coffee houses to restaurants and bars, with Tori being very free with his money in entertaining me. Finally, almost hesitantly, he mentioned that a military phone book from my unit would be of use to him, and he asked me to get a copy of it for him.

The phone book I provided for my friend Tori a few days later was gladly received, and Tori insisted that I accept several hundred dollars for all my trouble. This money, as was all money I received from Soviet Intelligence over the next 10 years, was turned in to the U.S. authorities. And so my conditioning continued, as Tori requested next a staff wiring diagram and then other apparently harmless, unclassified items. I was generously rewarded for all of them.

This conditioning was always low keyed. Tori would mention it would be nice to have such and such a publication. He was simply getting me in the habit of furnishing what he requested. Tori never introduced himself as a Russian or a Soviet intelligence operative. He never directly asked me to be a spy. At some unspoken point, all that simply became understood. His requests for material evolved gladly from simple unclassified information to ultimately the most sensitive classified information I could get my hands on. There was never any pressure on Tori's part, never a threat or hint of coercion. Neither was there need for cajoling or reminding me I had done little favors for him in the past and that this was no different.

Through a combination of friendship and financial remuneration, the relationship developed smoothly and progressively.

Finally, for the classified material, Tori made it clear there was no limit to the amount of money I could receive. Over the course of the operation, I received almost $25,000 from Soviet Intelligence. The succeeding months were busy ones for Tori and me, from passing messages to one another, via a series of signals marked on lamp posts, to receiving a rollover camera device so that I could film classified material without removing it from U.S. headquarters, to a series of dead drops used to exchange films and directions, to numerous clandestine meetings in remote parts of Bangkok, I was trained in the techniques of spycraft and encouraged to use my skills prudently but whenever possible.

[At this point in the hearing, Senator Cohen withdrew from the hearing room.]

Sergeant Smith. My training by Tori served as a primer on espionage. It ranged from the exotic—the Soviets provided me with a small transmitter with which I could signal Tori when I had material from him—to the mundane where I merely met him in a cafe and handed him material.

The rollover camera, which you have before you, is another proof of the lengths the Soviet Intelligence will go to obtain material. It is disguised as a notebook. I was instructed to carry a notebook in my pocket when I went to work for a couple of weeks. After it became natural for people seeing me with a notebook, I was to substitute the camera for the notebook and start copying material.

Tori was extremely sensitive of my situation, and he continually stressed the need for caution and security. He knew of U.S. security practices and spent hours discussing how I could defeat them. My relationship with Tori ended with my reassignment to Redstone Arsenal, AL, in August 1975, but my relationship with Soviet Intelligence continued.

In New York, through arrangements made by the Soviets before I left Bangkok, I met with a KGB agent I knew as "Bob." The arrangements for meeting Bob were that I was to sit tight in Alabama for approximately 90 days and then begin traveling to New York on the second Saturday of each month. I was to go to a pay phone booth near the American Stock Exchange on Greenwich Street and use the phone, or act like I was for 1 minute. I was then to walk a meticulously detailed route, ending up at a specific restaurant near a subway shop on Washington Avenue. I was to carry a certain specified magazine. I would be contacted by Bob and he and I would exchange innocuous oral phrases to introduce ourselves.

The Soviets have very detailed knowledge of New York City. Our meetings continued in New York City for a little over a year, with Bob tasking me to provide classified information regarding missile programs and other activities at Redstone Arsenal.

In response to my stated worries over repeated travel to New York City, Bob arranged a series of dead drops of hiding places in a churchyard cemetery near Fayetteville, TN. After approximately 1 year, in Alabama, I was telephoned by an unidentified Soviet who advised me that Bob had to return home, and I was not to travel to New York to meet Bob as planned. I was to wait until I was contacted at a later date and given new meeting arrangements.

Tori and Bob had both planned for such a contingency stating that in an emergency, the Soviets would contact my father in Buffalo, NY, to pass a message to me or to obtain a current address or phone number.

In August 1978, I was transferred to Germany and was not in contact with the Soviets at that time. However, the Soviets were able to trace me to my new assignment through a phone call to my father. My father, responding to a phone call from someone who introduced him as a friend of mine, gave them my address in Germany. Shortly thereafter, I found a message in my German mailbox requesting a meeting on the streets of Frankfurt, Germany, with a Soviet officer named Boris. With my new contact in Germany, the secret meetings, request for classified material and the other elements of espionage began again and continued until my next reassignment in August 1981.

At the time I received orders to the United States Readiness Command in Tampa, I was still in active contact with Boris. We arranged that I would travel to Mexico City after I relocated in Florida and meet my new KGB control agent at a pre-determined site. Again, I was given a meeting site previously selected by Soviet Intelligence.

I was, again, provided detailed instructions as to how I was to arrive and walk around the meeting site and how I would be approached by my new Soviet contact.

The meeting and my reunion with Bob, my former KGB Intelligence officer from New York City, went off exactly as planned. Once again, the spycraft cycle was activated, and I met with Bob a number of times in Mexico and Bogota, Colombia. The Soviet goal, as always, was for me to acquire for them the most potentially damaging classified defense information possible.

Bob and I had numerous discussions about meeting in the United States. However, Bob had a healthy respect for U.S. counterintelligence. He stated that it was simply too risky to meet with him in the United States. He stated I was too valuable to risk getting arrested. He did, however, suggest new dead drop sites and hinted about other communications systems. He did provide a new rollover camera and a specially constructed briefcase which I would use to take highly classified information from my office.

Senator NUNN. Is this the briefcase here?

Sergeant SMITH. Yes, Senator, it is.

Senator NUNN. Could you describe how that works for us?

Sergeant SMITH. As you can see, the upper portion of the brief case, which the Colonel is opening now, there is a concealed opening——

Chairman ROTH [interposing]. It doesn't work very well.

Sergeant SMITH. You have to pull out.

Senator GORE. It's Russian.

Sergeant SMITH. Yes, it is.

Senator NUNN. That is just for being able to transport secret documents in and out of the place and get by inspection; is that right?

Sergeant SMITH. Yes, sir.

Senator GORE. It is Samsonite.

Sergeant SMITH. That is an ordinary Samsonite that has been worked with.

During my next 10 years of activity, I had over 100 contacts with KGB agents in numerous countries on four different continents. Throughout the operation, I was repeatedly tasked by the Soviet Intelligence Service to provide highly classified material pertaining to U.S. military and defense policy, war plans, high technology, weapons research and development data, planning and evaluation of military exercises conducted by U.S. forces throughout the world, attitudes and perceptions of senior military officers, deployment of new weapons systems throughout the world and the ability of U.S. forces to conduct and sustain combat operations worldwide.

Senator NUNN. Let me ask a question there. Did the Soviets seem to know exactly what they wanted or were they basically using a shotgun approach saying go get anything you can? Were they analyzing what it was they actually wanted and tasking you to that purpose?

Sergeant SMITH. Senator, both of those conditions applied. At times, I was asked for very specific things, information on specific military exercises. At the time I was in Alabama, they were intensely interested in the development of the Pershing II missile which at that time was still in development stages. Their specific guidance was there intermittently, but they certainly wanted anything I could get ahold of that had a secret or top secret or some kind of classification caveat on it.

To discuss U.S. methods or actions used in counter-intelligence would be counterproductive to our own national interest today. I, therefore, have not addressed such matters and respectfully request that your questions also do not address them.

In closing, I believe that what we have and can say about my case is clear and ample proof, as I asserted earlier, of the pervasive, relentless and skilled assault on U.S. military members and Government employees by Soviet or Soviet-sponsored intelligence agencies.

Accepting that reality, there is no alternative to a strong personnel security program to protect those serving our Nation and ultimately, of course, our Nation itself.

That concludes my statement.

Chairman ROTH. Thank you, Sergeant Smith. We want to begin by expressing our appreciation for your being here and for the splendid work you are doing on behalf of our Government.

I would like to go back, if I might, just a moment. In your testimony, you said at the very beginning there was a very careful training period on how to spy. As I understand it, you were first given this notebook. Is this the actual notebook or one like it?

Sergeant SMITH. No, Senator, that is not the actual notebook. There are really two sets of those. There is a green set and red set. The ones I had were green. There is in DOD a common supply-issue-type notebook that says "Memo" on the front of it. The camera was designed to look exactly like that. The idea was you would carry the notebook around for a while.

Chairman ROTH. Carry it right in your——

Sergeant SMITH [interposing]. Yes

Chairman ROTH. You were so instructed to carry this for 2 or 3 weeks so your colleagues got used to seeing this notebook?

Sergeant SMITH. That's correct, Senator; yes.

Chairman ROTH. Afterwards, they substituted this camera for the notebook so there would be no suspicion on the part of those with whom you were working?

Sergeant SMITH. Yes, Senator, that's correct.

Chairman ROTH. This is a rather clever camera; isn't it? I notice this has a couple rollers here. Is this because you could take pictures of papers?

Sergeant SMITH. Yes, Senator. The way it operates, once you have the camera portion pulled out as you now have it, the upper portion there will close down; the roller will still protrude, but the upper portion will close and you just roll it over the page and it takes pictures as you roll it over the printed page.

Senator NUNN. You close it like that and roll it over like that?

Sergeant SMITH. Yes, Senator.

Senator NUNN. And it is taking pictures automatically?

Sergeant SMITH. Yes.

Senator NUNN. In other words, the roller triggers it?

Sergeant SMITH. Yes.

Senator NUNN. So it is to take pictures of documents more than anything else?

Sergeant SMITH. Yes, Senator.

Chairman ROTH. How many documents could you copy with this at one time? Do you have any idea?

Sergeant SMITH. I haven't used one of those for a number of years, but I believe in the vicinity of 60 pages with one little film cassette. You would have a number of little—I don't know if that has a piece of film in it or not right now. You would have a number of films you could carry, or cassettes, with it. When one ran out, you simply replace it. I think you can get 60 or 70 pages on one roll.

Chairman ROTH. You wouldn't use this when your colleagues were in your presence, would you?

Sergeant SMITH. No; a good spy wouldn't do that.

Chairman ROTH. The reason I raise this question why all this care then because basically you can only utilize this when nobody was around.

Sergeant SMITH. I think, Senator, in the business, you take every precaution that is reasonable and then you take some more because a little bit of paranoia is endemic to the business, so you get people used to seeing the briefcase. Before they give you a briefcase, they will say, do you normally carry a briefcase? If you say no, I don't normally carry a briefcase, they say, well, start for a while and let people get used to seeing you with a certain bulge in your pocket or carrying a black or brown briefcase for weeks or even months before they will even suggest substituting something for it. That is really good security practice.

Senator NUNN. I guess the main thing is, if somebody was coming in while you were doing that, you would snap it up, fold it up and make it look like a notebook.

Sergeant SMITH. I, obviously, wouldn't try to do that in the same room, but perhaps if they stepped out and you had field of vision of the hallway, you could see them coming and get that thing back in your pocket before anybody knew any different.

Chairman ROTH. Was there ever any evidence that the Russians were spying on you? How did they establish in their mind that you were reliable? Were you aware of any specific acts or actions on their part?

Sergeant SMITH. I was cultivated for weeks and months through going to the bars, talking about chess and such before even the request for a phone book was made. I have to assume that during that time, they were perhaps based on conversations the KGB agent was having with me, perhaps based on some surveillance assessing me before they made a pitch. I don't have direct knowledge that they followed me on the street.

Chairman ROTH. That is the question I was going to raise. As far as you could determine or tell, you were never aware of any such actions that they were following you or attempting to track you in any way to ensure your credibility.

Sergeant SMITH. Senator, no; I don't have any direct evidence of that. I am very certain they did it.

Chairman ROTH. But basically, as far as you could tell, they relied on developing this friendly, cordial relationship.

How did that work when the agents were changed? You had Tori initially, but when you were reassigned, they brought in another agent. Was there any period of time in which they tried to rebuild that relationship or immediately did the new man begin asking you for material?

Sergeant SMITH. No, they began immediately. They, in my case, started out with friendship and money. This is common, but not always the way they do it. After a period of time, they remained friendly. They will do whatever works, but as I mentioned before, at some unspoken point, you're theirs; they know you're theirs; you know you're theirs, and you are really doing business.

When I went to a new agent, Senator, we were doing business. They still called me by my first name and that sort of thing, but business after the first few months was obviously, although not so spoken, the centerpiece of the arrangement.

Chairman ROTH. In other words, you were hooked, so to speak, and they relied on that to continued the so-called working relationship?

Sergeant SMITH. Yes; exactly, sir.

Chairman ROTH. Never were any kind of threats or blackmail or anything of that sort from any of your contacts?

Sergeant SMITH. No; I don't think, Senator, in my case that would have made sense for them to do. There were plenty of documented cases where people have had, say, relatives in countries behind the Iron Curtain, something they could be blackmailed on. Those are things they do use. They just did not choose to use those on me

The Soviets rely on money, ideology, compromise and ego. The acronym for that is MICE, and they would use any one or, preferably, a combination or all of those to get to people.

In my case, they were using money and ego through the friendship.

Senator NUNN. What does the "I" stand for?

Sergeant SMITH. Ideology.

Senator NUNN. Compromising and ego?

Sergeant SMITH. Yes.

Chairman ROTH. When the new agents took over, was there any evidence they were carefully briefed about you and your background? Was the new agent pretty familiar with you?

Sergeant SMITH. Oh, yes; yes, Senator; yes.

Chairman ROTH. It was obviously a very well-planned operation.

Sergeant SMITH. Yes; they had to be prepared on me from knowing me walking down the street somewhere, all I was supposed to do was walk around a certain block and stop in front of a certain restaurant in a particular place in New York or Mexico City. It was up to somebody else to recognize me, approach me, say a certain key phrase, and I responded with a phrase to verify him, and then we got down to business.

I mentioned that they were using, in my case, money and ego. They continued that from agent to agent and no change to that.

Chairman ROTH. My last question, and then I will ask Senator Nunn to proceed. What was it initially that made them feel that you were a possible aid? What was it you said or did that gave them the idea that here was a possible person who might cooperate?

Sergeant SMITH. To begin with, Senator, I was working at a Military Systems Command, Thailand, which was a good target for them. There was a lot going on there, so they were interested in having sources at a place like that.

Second, through my interest in chess and frequenting of this European bar, they had a scenario where they could approach me, they thought, I think safely without showing themselves. It was out in the open somewhere and not at the compound.

When they began talking to me up—they think all Americans are money-hungry. They believe money talks; that all Americans believe that. That is something, I think, they would use on anybody.

They, obviously, believed I was susceptible there. They thought if I could be turned, I would be smart and useful to them, and once I had given them the phone book and a few seemingly innocuous things based on friendship, which was their major, at least initial, tactic, they were counting on me realizing that I had done something wrong and was now hooked, so to speak.

I think that is kind of a long answer, but that is the answer to your question.

Chairman ROTH. Senator Nunn?

Senator NUNN. Thank you, Mr. Chairman. How much money did you receive during this? Did you keep close count of it?

Sergeant SMITH. It was approximately $25,000.

Senator NUNN. $25,000. Was that negotiated or was that simply you brought them information and they gave you whatever they liked in terms of money? Did you say this was worth so much? Was there a point rating going on or simply whatever they gave you?

Sergeant SMITH. There were times when both of those situations applied. I did complain at times or say that such and such was worth something and other times they just gave me an envelope.

Senator NUNN. Did you usually complain after the fact they paid you or before you delivered, did you say this is worth $5,000 or so forth?

Sergeant SMITH. Senator, my tendency would be to do it beforehand.

Senator NUNN. More plausible that way?

Sergeant SMITH. Yes.

Senator NUNN. More American. [Laughter.] Was there any significance to the fact that you were approached in Thailand, a foreign country?

Sergeant SMITH. I don't think there is any special significance as far as I go. I was simply a target of opportunity, appeared friendly and approachable. I was felt out, assessed for potential value and cooperativeness for a long time before they considered using me. I think the real significance is that the KGB in size is a huge organization and is much greater in size than the sum of all the American activities whose function it is to counter the KGB. That is a documented fact.

It is also significant in that there is no area of the world that is denied to them or that doesn't have their interest. That is also documented.

I would commend anybody reading either John Barron's books on the KGB, one called "The Secret Work of Soviet Agents," and the other called "The Hidden Hand," more recent. So we have to assume on any given day, many Americans and others from Western nations are being cultivated and assessed for potential use by the KGB. Of these, some will be selected for a pitch, because I was.

This is an ongoing war; predates the end of World War II. It is proven immune from attack, arms agreement, leadership changes and everything else, but to suggest there was anything extraordinary about my being pitched by the KGB totally misses the point because it happens every day.

Senator NUNN. You mentioned your acquaintance by the name of Tori knew of U.S. security practices and spent some time with you in discussing some ways to defeat those practices. Could you give us a little more detail of what he seemed to know and what he advised in terms of defeating U.S. Security practices?

Sergeant SMITH. Yes, Senator. The Soviets are aware of periodic security inspections conducted by the Army. They are aware of the various types of security clearances and background investigations necessary to acquire clearances. They are aware of registered mail procedures, of methods used to control classified documents, of controlled access areas. They are aware of the Achilles heel represented by copying machines.

In circumventing security, the Soviets keyed on acting natural, using extreme caution and finding plausible ways to be alone with classified material. In my case, they seemed to have a great deal of confidence in my judgment and ideas, although I was constantly told to be careful. At times, used to their own system, the Soviets were surprised by certain things, such as how pervasive these various unsupervised copiers are in the absence of political indoctrination officers.

Senator NUNN. You mentioned the marking of lamp posts, so forth. Could you tell us a little bit of what you mean by dead drops?

Sergeant SMITH. A dead drop is simply a preselected site for leaving messages, film, documents or receiving the same. It is dead in the sense that material is passed without human contact. A knot hole in a tree; ledge in a phone booth; fence post; under leaves by a lamppost are all examples of dead drop sites.

Typical use of a dead drop might run as follows:

By signals made with chalk on a lamppost, you indicate that you have film or material to be delivered. You get a return signal and you are given the go-ahead to deliver to the dead drop. You already have a date and time for delivery following your returned signal. You place the film in a preselected container, perhaps an old tin can crushed around the film or empty cigarette pack. The film should be wrapped in plastic to protect it from moisture, protecting the bits of information. You deliver it to the dead drop. You mark the lamppost to indicate the material is at the dead drop. You wait an hour; then another signal that the material has been received. If there is no signaled receipt of material, you retrieve the material and begin the process again.

Senator NUNN. If you were advising other military personnel in similar situations or giving any advice to those responsible in our Government for personnel security, based on your experience over 10 years and your extensive contacts with the KGB, what would your advice be?

Sergeant SMITH. Senator, I think in a large way, that is a question for generals and policymakers, these people whose business it is to decide what is best for the whole force. My function in working for counterintelligence was to focus intently on a single data or a single tree, so to speak, and to know every nook and cranny of that so we can make it go our way. But that kind of experience, which did not only call for looking at the whole forest, it precluded it.

So in some ways, although I have a lot of experience, it is not the right kind of experience for people whose job it is to know the big picture and who should recommend policy.

Senator NUNN. How about just from the point of view of someone in a similar position to you in the U.S. Army?

Sergeant SMITH. Yes, sir, I would recommend we explore ways to increase public awareness both in the Army and out of the real and pervasive threat of the KGB, Soviet intelligence agencies in countries they control. People need to know it is not a spy novel or James Bond movie world we are talking about today; it's the real world. And while certain circumstances in my case may be unusual, the fact that I was approached is common. If we can increase awareness of that fact, of being wary enough to report any possible contact by hostile intelligence of not being sucked in, so to speak, by small favors to a friend, of not letting your weaknesses dig you a bigger hole, then we can come a long way.

Preventive medicine, which is security and awareness, is the best approach.

Senator NUNN. Let me ask you a question. It is a bit hypothetical. If you had not been a double agent, if you had not been cooperating with our own Government, and if you had decided that you really did want to betray our Government and receive money for that betrayal, do you believe you could have gotten away with it based on our personnel security that you observed?

Sergeant SMITH. I don't think that I would have been caught unless I made a mistake. It is important to understand that there is really no fail-safe safeguard if a spy is cautious and retains plausible behavior. Of course, American penetration of KGB activity could have led to my being caught, or someone in similar circumstances. Routine surveillance of known KGB operatives might have surfaced me, had my own countersurveillance and KGB countersurveillance not been effective.

As you mentioned, Senator, that is a hypothetical question and other things, such things as psychological pressure of being a Soviet spy in American uniform, I would think eventually this might lead to a foolish error or confession or emotional breakdown.

In many cases, that is so. In my case, of course, I didn't have that pressure.

Senator NUNN. Sergeant, we appreciate very much not only your appearance today, but what you have done for the Army and your country. Mr. Chairman, that is all the questions I have.

Sergeant SMITH. Thank you, Senator.

Chairman ROTH. Thank you, Senator Nunn. Senator Gore?

Senator GORE. Thank you, Mr. Chairman, Very briefly, I want to add my statement of thanks to you, Sergeant, on behalf of an awful lot of people who admire your courage and persistence in what was a very difficult period of time. Your counterintelligence work lasted for quite some time; is that correct?

Sergeant SMITH. Yes, sir.

Senator GORE. Over how long a period of time?

Sergeant SMITH. Over 10 years.

Senator GORE. I take it that the central meaning of your testimony, is very simply that the Soviet espionage threat is pervasive and broadly based. It is aimed at conceivably any member of the U.S. military, because at the time you were approached you didn't have any special access to materials and you weren't clearly identifiable as someone with access to secrets; is that correct?

Sergeant SMITH. That's correct, Senator. They begin by fishing and see what they can get.

Senator GORE. At the time you were contacted, did you have security clearances?

Sergeant SMITH. Yes, I did, Senator.

Senator GORE. Secret, top secret?

Sergeant SMITH. I did have top secret clearance when I was contacted. That was not something that was known to them, however.

Senator GORE. So far as you know?

Sergeant Smith. So far as I know, Senator.

Senator Gore. I was intrigued by your reference to Fayetteville, TN. Many times I never thought of it as a dead-drop site, but just out of curiosity, was its proximity to Redstone the reason Fayetteville was selected?

Sergeant Smith. I'm sure, Senator. Yes, the proximity. It was a fairly rural area. I didn't select it. I had to ask the Soviets——

Senator Gore [interposing]. Just for the record, it is a beautiful place, don't you think?

Sergeant Smith. Yes, I do, Senator.

Senator Gore. I would like to thank you again. The chairman and Senator Nunn covered the area very, very well. I, again, thank you for your patriotism and dedication. Thank you, Mr. Chairman.

Chairman Roth. Sergeant Smith, you have our gratitude. You are known for your brightness, but a pretty good politician, too. We do appreciate you being here today.

We will have to clear the room again since there are no more questions. I would ask that everyone, once again, leave the hearing room.

Senator Nunn. Mr. Chairman, when we return, we will have two more witnesses. One will be a staff investigator who will talk about the Veliotis case, background on that and the other will be the FBI and that would conclude for today.

Chairman Roth. I would express my appreciation for the fact Senator Nunn has also agreed to continue chairing the remainder of the meeting. I have another committee meeting.

Senator Nunn. Thank you, Mr. Chairman. We have questions for General Scanlon. We will submit those for the record. Thank you, General Scanlon.

General Scanlon. Sure.

Chairman Roth. The room will please be cleared.

[Brief recess. Senators present at the time of the recess: Senators Roth, Nunn, and Gore. Senators present after the recess: Senator Nunn.]

Senator Nunn. First, let me thank the news media and members of the audience for your cooperation in accommodating the special arrangements with the previous witness. We try not to have the screen unless it is absolutely essential. We went over this with the Army in great detail in a number of different meetings and concluded their reasons for requesting identity protection were valid. They were valid reasons that satisfied me, and that is why we proceeded under that at the Army's request.

Our next witness is Mr. Fred Asselin who has a thorough and detailed statement on the Veliotis case but has summarized it in what should take about 10 minutes. Fred is one of our valued staff members, and he will take the oath as other witnesses.

Do you swear the testimony you give before the subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. Asselin. I do.

Senator Nunn. State your name and position for the record.

TESTIMONY OF FRED ASSELIN, STAFF INVESTIGATOR FOR THE MINORITY, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

Mr. ASSELIN. My name is Fred Asselin. I am on the minority staff of the Senate Permanent Subcommittee on Investigations. I have worked on or with the subcommittee staff since 1969.

I have a prepared statement which I request be printed in the hearing record as read. I will read a shortened version that will last about 10 minutes.

Senator NUNN. The acting chairman has read your detailed statement. We will put it in the record, without objection.

Mr. ASSELIN. In its preliminary investigation into the efficiency and effectiveness of the Government personnel security programs, the minority staff examined the procedures followed when immigrant aliens and recently naturalized citizens apply for security clearances.

The fundamental question the staff sought to answer was how thorough an examination of the applicant's past is accomplished concerning his life in the country of his birth and in other foreign nations where he may have lived. The answer is that in many instances, information provided by the applicant is not verified. Obstacles to more effective verification include:

One, to varying degrees, foreign nations are not tolerant of trained American agents doing direct inquiry within their borders.

Two, the actual inquiry is sometimes conducted or directed by American officials with limited investigative training or who have other priorities and, therefore, do not bring to personnel security investigations the sense of urgency and timeliness needed.

Three, records in some foreign nations are not always accessible, or well maintained, or as precise as desired.

Four, clearance applicants from communist nations and certain Third World nations, such as Iran, pose a problem for personnel security programs because it is generally not possible even to attempt to verify their assertions about their past.

Several of the problems associated with investigating foreign nationals were seen when Panagiotis Takis Veliotis, a citizen of Greece and Canada and later the United State, applied for secret and top secret Defense Department clearances and a "Q" access authorization from the Energy Department.

Veliotis left his native Greece in the early 1950's and emigrated to Canada where he became a shipbuilding executive and a Canadian citizen. In late 1972, he emigrated to the United States where, as a senior official and member of the board of directors of General Dynamics, he was in charge of certain military and nuclear propulsion programs, including construction of Trident and nuclear attack submarines. He also became a naturalized U.S. citizen.

In one period during his 9-year tenure with General Dynamics, Veliotis allegedly participated in a $2.7 million kickback scheme. Indicted by a Federal grand jury in the Southern District of New York, Veliotis fled this country and is now living near Athens as a fugitive.

The minority staff felt the Veliotis case would be informative to the subcommittee members because it demonstrates not only the inherent difficulties in conducting investigations of immigrant aliens; it also reveals certain procedural inadequacies in the operations of the Government agencies involved in the inquiry into Veliotis' past.

I have prepared a chronology of developments affecting Veliotis' life. I request that the chronology be printed in the hearing record and the documents from which the chronology is drawn be received as public exhibits to these hearings and stored in the subcommittee files.

[The chronology referred to was marked "Exhibit No. 12" for reference and is found on p. 111. A summary statement by the Energy Department apparently used by the Department in adjudicating Veliotis' 1977 application for a "Q" access authorization was marked "Exhibit 13" for reference purposes and is found on p. 149. Other documents from which Mr. Asselin's summary chronology was drawn were marked "Exhibit 14" and may be found in the files of the subcommittee.]

Mr. **Asselin**. I will now read a summary of the highlights from the chronology.

The personnel security procedures followed by the executive branch regarding Veliotis were inadequate and demonstrate the need for more thorough inquiry into the backgrounds of immigrant aliens and recently naturalized citizens who apply for Defense Department secret and top secret clearances and Energy Department "Q" access authorizations.

Veliotis, who in 24 years rose from a marine draftsman in Greece to become a senior manager and officer in this Nation's largest defense contractor firm, was given secret and top secret clearances and a "Q" access designation. He was placed in charge of two major shipbuilding facilities in the United States both of which did classified defense and nuclear work. He was selected at a time of labor-management unrest to manage construction of Trident submarines, nuclear-powered vessels that comprise a substantial portion of the American strategic weapons capability, and Los Angeles class SSN nuclear attack submarines.

Yet with these important responsibilities, little was known about Veliotis' life in Greece, beginning with his reported birth in 1926 until 1953 when he reportedly emigrated to Canada from Piraeus, the port city near Athens. American authorities were able to verify few assertions that Veliotis made about his past.

For example, of the individuals interviewed as references for Veliotis in his personnel security investigations, none of them knew him in Greece or prior to the 1953 emigration date he gave on several U.S. Government documents.

There was no original documentation provided certifying to the facts and place of Veliotis' birth.

Investigators were unable to verify Veliotis' assertions about his formal education and his reported service as an officer in the Greek Navy during World War II. In addition, Veliotis claimed on his Government personnel security forms to have earned an engineering degree from, and been commissioned as an "engineer officer" by, the Royal Naval Academy of Greece. However, a highly reliable confidential source, who has seen FBI files on this matter, has informed the minority staff that the bureau determined that while Veliotis did enroll in the naval academy, he did not graduate, thus casting more doubt upon his assertions about his formal education and military record.

Information was also developed by the FBI indicating that Veliotis was convicted of a money order violation in Piraeus in 1954, and sentenced to 45 days in jail. This information was never reconciled with Veliotis' frequent assertion made in DOD and INS papers that he emigrated to Canada in 1953.

In addition to these questions about Veliotis' past, there were other questions about his career once he emigrated to North America.

For example, in January of 1973, when he took over as president/manager of the General Dynamics Shipbuilding Division in Quincy, MA, he apparently had no U.S. security clearance, even though classified military and nuclear work was being performed there. A year went by before he obtained a U.S. secret clearance. There is no evidence that Veliotis had a Canadian reciprocal secret clearance during that first year at Quincy.

The Defense Department, responding to its own rules prohibiting immigrant aliens from handling top secret information or presiding over top-secret facilities, reduced the facility clearance of the Quincy shipyard from top secret to secret. The shipyard also posted photographs of Veliotis, and three other immigrant aliens, who comprised the Veliotis management team, so that guards would not mistakenly allow them access to sensitive areas.

Senator NUNN. In other words, the guards, when the head of the shipyard comes up, are supposed to have a picture up there saying he is not admitted.

Mr. ASSELIN. In front of the sensitive areas.

Senator NUNN. He was heading up the shipyard.

Mr. ASSELIN. He is also, from all reports, a very imposing figure himself.

Senator NUNN. He is the one paying the guards; right?

Mr. ASSELIN. Yes.

Senator NUNN. He is the one hiring the guards?

Mr. ASSELIN. Yes.

Senator NUNN. He is the one that can fire the guards?

Mr. ASSELIN. Presumably, yes.

Senator NUNN. They are supposed to be the ones who say, "Sorry, you can't have access"?

Mr. ASSELIN. Yes.

Similarly, DOD officials, continuing to be concerned about the security problem caused by Veliotis, discussed downgrading from top secret to secret the clearance level of the General Dynamics Corp. itself. This was because Veliotis was also a vice president of General Dynamics Corp. and DOD required that a firm's clearance be no higher than that of its management. DOD provided no evidence that this action was taken against the corporation, however.

In 1977, when Veliotis was made general manager of the Electric Boat Division in Groton, CT, Veliotis' immigration status and lack of a top secret clearance again triggered a downgrading of facility clearance. DOD reduced the facility clearance of the Groton yard and the nearby Quonset Point facility in North Kingstown, RI, from top secret to secret.

In 1973, when he was president and general manager of the Quincy yard, Veliotis made a trip to Russia and did not report it to Federal authorities. This was in violation of the DOD Industrial Security Manual. In 1977, when he applied for a "Q" access authorization from the Energy Department, Veliotis' unreported Russian trip was known but the Energy Department did not question him about it and approved his "Q" access request.

The Energy Department had information in 1977 from the FBI indicating that in June of 1954, Veliotis was convicted and sentenced to 45 days in jail for money order fraud in Piraeus, Greece. The Energy Department did not question Veliotis about this apparent derogatory information, nor did the department seek to reconcile the date of the reported conviction in Piraeus—1954—with the frequently made assertion by Veliotis in Government documents that he had emigrated to Canada in 1953. Giving a "Q" access authorization to a foreign national is rarely done. Today, for example according to the Energy Department, only four foreign nationals have such a clearance. A senior Energy Department official has acknowledged that the procedures that led to Veliotis' "Q" access were inadequate.

In May of 1980, Veliotis, by this time a naturalized American citizen, was given a top secret clearance. But no personnel security inquiry was conducted to justify the granting of the top secret clearance to Veliotis. Defense officials asserted that the required DOD inquiry was waived because Veliotis already held an Energy Department "Q" access authorization, but the investigation preparatory to the "Q" clearance turned up a substantive derogatory, had unreconciled inconsistencies regarding crucial dates in Veliotis' past and, therefore, may itself have been flawed. The Energy Department has been unable to find evidence to indicate that DIS followed the required procedures preparatory to waiving the need for a background inquiry. DIS said it has such evidence.

Questions have been raised about Government operations in 1982 when a Federal grand jury in the Southern District of New York began to develop information that ultimately would lead to indictment of Veliotis and a General Dynamics colleague on charges of having accepted $2.7 million in kickbacks from a subcontractor. According to information given the subcommittee by General Dynamics officials, they were informed on February 5, 1982, by a Federal prosecutor that Veliotis was a subject in the grand jury probe and that General Dynamics should examine Veliotis' "sources of income from all over the world."

It is a serious matter for anyone to be a subject in a Federal grand jury inquiry. It is particularly serious when that person is a corporate officer and an operational manager in the world's largest defense contractor, General Dynamics, and when that person has a top secret Defense Department clearance and a "Q" access authorization from the Energy Department. A man alleged to have received millions of dollars in kickbacks might constitute a security risk; at least DOD and Energy Department personnel security experts should have been put on notice that such a potential problem existed.

There is no indication in the information given the subcommittee by DIS that DIS was advised of Veliotis' potential security problem.

Similarly, he remained in his senior position with General Dynamics following the February 5 notification by the Justice Department.

Veliotis was reappointed as executive vice president by the General Dynamics board of directors on May 6, 1982. That same month, Veliotis resigned from General Dynamics. It should be noted that a condition of defense contracts is that the contractor is obligated to alert the Pentagon to any untoward conduct on the part of a cleared employee.

Veliotis' employment form, the original job application questionnaire he submitted to General Dynamics in late 1972, is inexplicably missing from the firm's files, according to General Dynamics' general counsel.

The FBI has not cooperated with the subcommittee in the Veliotis matter. The FBI twice conducted background investigations on Veliotis—in 1973 when it looked into his past in Canada in connection with his request for a DOD secret clearance, and in 1977 when it looked into his past in connection with his request for an Energy Department "Q" access authorization. The subcommittee has asked the FBI for its Veliotis personnel security files. The bureau has refused to turn them over or to answer questions about information contained therein.

The minority staff submits to subcommittee members for their consideration the following preliminary findings, conclusions and recommendations for corrective action:

One, Veliotis, who is a fugitive charged with having participated in a $2.7 million kickback scheme while having control of a shipyard that worked on military and nuclear propulsion programs, represents a potential breach of national security of serious dimensions. The executive branch should conduct an investigation to determine the facts of his past. When the results of that inquiry are available, the executive branch should then consider the possible need for a damage assessment.

Two, inadequate effort was made to vet Veliotis both prior to and during his service in sensitive national security positions.

Three, more comprehensive and thorough inquiry is needed to verify key assertions made by immigrant aliens and recently naturalized citizens about their past in foreign countries when they apply for security clearances.

Four, the Departments of State, Defense, and Energy, the Office of Personnel Management, and the intelligence community, should work together to devise a more reliable system of doing personnel security checks in foreign countries on immigrant aliens and recently naturalized citizens who apply for U.S. clearances.

Five, in the Veliotis case, clearance applications were approved in the face of unverified and possibly contradictory assertions by the applicant. In summary, adjudicators when in doubt approved his clearances. Another approach was called for. Instead of giving applicants the benefit of the doubt, Government should put the burden of proof on them. When they found that they could not verify Veliotis' assertions about his own past, the Pentagon and the Energy Department should have asked him to produce evidence to corroborate his resume in the form of diplomas, papers certifying to his commission in the Greek Navy, military discharge documents, a birth certificate. If, after giving the applicant the opportunity to support his own case, the documentation is still incomplete or otherwise unverified, the Government should deny the clearance.

That completes my statement, Senator.

Senator NUNN. Thank you. I have one question. In your Recommendation No. 1, you state, "Veliotis, who is a fugitive charged with having participated in a $2.7 million kickback scheme while having control of a shipyard that worked on military and nuclear propulsion programs, represents a potential breach of national security of serious dimensions."

Continuing, "The executive branch should conduct an investigation to determine the facts of his past." Are you saying the executive branch has not conducted a national security type investigation of Veliotis in spite of all that has happened?

Mr. ASSELIN. That is our understanding, unless they are not telling us. That's exactly right. What we are recommending is the kind of inquiry that should have been done initially. If they determine he is telling the truth, there may not be need for damage assessment. It seems to us they need to find out who the man is before they go further.

Senator NUNN. You don't think they have done that? At least in your conversations with various agencies in your investigation, which is reflected here, you have not found a true national security investigation of Veliotis, even to this day?

Mr. ASSELIN. From what people told us, no. We have raised this issue with the Department of Defense and the Department of Energy. We tried to raise it with the FBI and Department of Justice. In each case, we were met with a lack of enthusiasm for the idea. The principal problem seems to be that there is no mechanism whereby they could go forward with such a project.

Senator NUNN. Meaning what?

Mr. ASSELIN. The executive branch responds by asking, "Well, who is going to conduct this investigation?"

Senator NUNN. What they have done is basically conducted the fraud, the money part of it, the cheating part of it, various allegations against General Dynamics, all of that we assume is being investigated; is that correct?

Mr. ASSELIN. Ours has been somewhat of a narrow inquiry, Senator. I didn't get into the overrun issue.

Senator NUNN. If there are investigations, they are in that area; not the national security area. You are not saying he breached national security; you are not alleging that. You are saying nobody really knows at this point; is that right?

Mr. ASSELIN. That is exactly right. The first thing we recommend that Senators consider is that there be a real vetting of the man to find out if he does have a military record; if he has graduated from these various schools. There are many questions raised about the man, and then when they have done that, find out if a damage assessment is called for.

Senator NUNN. Has anyone indicated there has been an extensive check into the trip to the Soviet Union that was not properly reported?

Mr. **Asselin**. There is no evidence. The reason we raise that, that existed and should have checked that out.

Senator **Nunn**. They still haven't checked that out?

Mr. **Asselin**. I don't know what they have done. We have raised the issue with them several times.

Senator **Nunn**. Them being?

Mr. **Asselin**. Various executive branch agencies. We have yet to find a receptive response that someone should find out who this gentleman is. It may well be everything he put in his forms is accurate. The inconsistencies could be ironed out, and he may have an explanation for everything.

Senator **Nunn**. There are a number of inconsistencies?

Mr. **Asselin**. Yes.

Senator **Nunn**. For which you have no answer.

Mr. **Asselin**. The Government has no answer, and the Government is not being receptive to our recommendation.

Senator **Nunn**. Thank you very much.

[The chronology, Exhibit No. 12 submitted by Mr. Asselin, and Exhibit No. 13 follow. The documents from which the chronology was drawn were marked Exhibit No. 14 and may be found in the files of the subcommittee.]

Exhibit No. 12

CHRONOLOGY

This is a chronology of pertinent events concerning Veliotis. Most entries in the chronology are supported by one or more documents provided, according to proper and established procedures, by the Departments of Defense and Energy and the General Dynamics Corporation. Footnotes cite all factual sources. Comments and interpretations are my own.

August 11, 1926--According to papers filed with the Immigration and Naturalization Service and the Departments of Energy and Defense by Veliotis, he was born on this day in Kranidion, Greece.[1] As will be demonstrated in this chronology, no original documentation stemming directly from Veliotis's actual birth has been cited or located. As a consequence, there has been only limited corroboration of Veliotis's account of the place and date of his birth.

1944 to 1947--According to Veliotis's responses to an Energy Department personnel security questionnaire, Veliotis served during this period in the Greek navy.[2]

1947 to 1953--Veliotis, in the same questionnaire, said he was employed during this period by E. G. Veliotis, reportedly his father, in a marine engineering firm at 34 Afentouli Street, Piraeus, Greece.[3]

1953--At some point in this year, Veliotis left Greece and entered Canada where he went to work for Davie Shipbuilding Ltd., of Quebec, a subsidiary of Canada Steamship Lines.[4] At least that is what he wrote in the Energy Department questionnaire and in other documents about his emigration to Canada. Questions remain, though, about his life in Greece and the reliability of his recollections of his activities there. For example, in his entry in Who's Who for 1982-1983, Veliotis added to the information about his military record and other activities in Greece by asserting that he "served as an officer Royal Hellenic Navy, World War II," and also indicates that he earned a "B. A." degree from St. Paul College in Greece, did graduate work at the National University in Athens and earned a degree in engineering from the Royal Naval Academy of Greece.[5] At the time of his leaving the Navy, Veliotis would have been 21, having earned a "B. A." degree five years earlier at the age of 16. Unless he conducted some of his studies while in the service, he was able, in the six years from 1947 to 1953, to do graduate work and complete requirements for a degree in engineering while, at the same time, he was employed by E. G. Veliotis in the marine engineering firm in Piraeus. His 1953 arrival in Canada is attested to by Veliotis several times, not only in the Who's Who entry but in papers he filed with the government. Nineteen fifty-three is also the date of Canadian entry he gave General Dynamics.[6] However, federal authorities believed that Veliotis was in Piraeus before the "Court of Misdemeanor" on June 7, 1954 where he was sentenced to 45 days in prison for money order fraud.[7] In addition, Veliotis answered "no" on government forms asking if he had been charged or convicted of a crime. As will be seen in this chronology, the inconsistencies in Veliotis's accounts of his own past never were resolved. But they did not stand in the way of his obtaining U. S. secret and top secret clearances and a Department of Energy "Q" access designation.

November 6, 1955--Veliotis married Vasiliki Bessie Anastosios Charkas in Montreal. The couple lived in Canada. A son, Eleutherios George, was born in 1960 and a daughter, Joanna, was born in 1961. Veliotis and Charkas were divorced in 1969 in Quebec City.[8]

1962--After several years in the employ of Davie Shipbuilding in Quebec, Veliotis was promoted to Director and General Manager of the firm. According to a resume on himself, Veliotis's position as President and General Manager of Davie Shipbuilding gave him "chief responsibility for entire shipyard," where the work was performed by 2,600 employees and included the building and repair of "bulk carriers, tankers, freighters, drilling rigs, naval ships and tie breakers."[9] David Lowery, who was Vice President of Davie's parent Canada Steamship when Veliotis ran the shipyard, had praise for his management skills. "Every year he ran the yard, we made money," Lowery told Forbes in January of 1984.[10]

September 25, 1967--E. S. Perkin, Director of Industrial Security, Canadian Department of Defense Production, wrote G. L. C. Bates, Davie's Chief Security Officer, to note that Veliotis "has been checked from a security standpoint" and that he is qualified to have access to information of "a secret nature."[11] Perkin said, "Where it is necessary for him to have access to classified information resulting from officially classified contracts or negotiations, such access may be allowed up to and including that of a secret nature." So far this is the only document provided the Subcommittee which attests to the assertion that Veliotis had a Canadian secret clearance. This letter, five years old at the time Veliotis took charge of the Quincy shipyard, may have been the sole basis for the belief in 1972 that Veliotis had a Canadian secret clearance. To have received a secret clearance in Canada in 1967, applicants would have submitted to two kinds of tests. First, the RCMP Security Service checked its own files for relevant information on the candidate, his relatives and close friends. Second, the RCMP initiated a fingerprint check of criminal records. No further inquiry was done, although a field investigation could be initiated for cause. Based on the information it collected from these investigations, the Security Service assessed the candidate from a security standpoint and advised the relevant government department on whether or not to issue a security clearance.[12]

November 27, 1967--The Naval Material Command headquarters in Washington, D. C. gave an interim top secret facility clearance to the General Dynamics shipyard in Quincy, Massachusetts because of the classified "technical services" it performed in support of the Vietnam war. Requesting that such a clearance be given the Quincy facility, L. Z. Robitaille of the Naval Ship Systems Command pointed out that the higher clearance was needed "to avoid crucial delays in contract performance."[13]

January 1971--The U. S. Navy began issuing contracts for the construction of 41 SSN 688 attack submarines. Tenneco, Inc., owner of a shipyard in Newport News, Virginia, was to design the vessel and produce 17 submarines. The Electric Boat Division, located in Groton, Connecticut, which was a subsidiary of General Dynamics Corporation of St. Louis, was awarded a contract for seven 688s at this time. Eleven additional 688s were to be constructed under the terms of a contract awarded to Electric Boat in the fourth quarter of 1973.[14] It is informative to note the key role played by General Dynamics in the American submarine program. The U. S. Navy's submarine forces consist of two principal categories: ballistic missile submarines (SSBN), and attack submarines (SSN). The SSBN category includes the Trident nuclear-powered submarines, which are built by General Dynamics's Electric Boat Division in Groton. The SSNs, referred to as nuclear-powered attack submarines, are built at the Electric Boat yard and at Newport News.[15]

April 22, 1972--Veliotis married Paulette Marie Emmasimone Dupuis in Quebec.[16] At some point around this time Veliotis reportedly also became a naturalized Canadian citizen.

1972--General Dynamics received a contract to build 10 liquefied natural gas vessels at its shipyard in Quincy, Massachusetts. Earlier in 1972 General Dynamics had considered closing the Quincy Shipbuilding Division because of poor profitability but late in the summer a Burmah Oil Co. Scotland unit had ordered three tankers costing $268.7 million for delivery by 1977. This caused an immediate change in outlook for the facility. The Burmah tankers were to be designed to haul liquefied natural gas from Algeria to the U. S.[17]

October 31, 1972--Now that the Quincy shipyard had been awarded the contract to build the vessels for liquefied natural gas, General Dynamics began the task of bringing in a new executive to run the Massachusetts facility. Paul R. Ray & Company, Inc., an executive search firm located in Fort Worth, was engaged to identify candidates for the job. On the above date, Paul R. Ray himself wrote Algie A. Hendrix, Corporate Vice President of General Dynamics for Industrial Relations, to report on how the executive search was progressing. Of the 50 executives mentioned in Ray's letter--from firms that included Newport News Shipbuilding & Dry Dock Co., Bethlehem Steel, Avondale Shipyards, Maryland Shipbuilding and Drydock Co., Todd Shipyards, Bath Iron Works, National Steel Shipbuilding, American Shipbuilding, Lockheed Shipbuilding, Alabama Dry Dock & Shipbuilding Co., three consulting companies and one university--only two men were considered to be viable candidates. The other 48 were not in the running, Ray said, because 1) they expressed no interest in taking over at Quincy; 2) they were adjudged to be unqualified; or

3) they had been rejected for reasons unstated by Ray but which, in several cases, may have had to do with instructions from General Dynamics senior management. Of the final two candidates, one had asked to be taken out of contention at the 11th hour. That left only one. However, Ralph Cyphers, an assistant to Paul R. Ray, had evaluated the final candidate and, according to a memorandum of October 27, 1972, had reached the conclusion that, while interested in the Quincy post, he had somewhat limited shipbuilding experience and, equally significant, he would bring to the Quincy yard only himself--and not a management team. The memorandum warned:

> In employing Mr. ________ the company would be obtaining one individual managerial talent. There would be risks involved in obtaining additional managerial talent compatible with Mr. ______ and in time to manage future business.

It seems to be apparent, then, at least in the minds of Paul R. Ray executive search specialists, and possibly in the minds of General Dynamics officials, that not only was a new chief executive needed for the Quincy yard, but a new management team was required as well--a group of executives who had worked together in the past and who had a proven track record.[18]

November 7, 1972--Eight days after the executive search report from Paul R. Ray & Co. to General Dynamics, the company had decided to hire Veliotis to head the Quincy shipyard. General Dynamics had also decided to retain other members of the Veliotis management team from Davie. In a "Dear Takis" letter of the above date, Hilliard W. Paige, President of General Dynamics, wrote to Veliotis to say, "we are most pleased that you have accepted our offer to join General Dynamics Corporation." Paige went on to say:

> As you know, we have made an extensive but unsuccessful search throughout the United States for the shipbuilding managerial talent necessary to do the job at our Quincy shipyard. The extraordinary record of profitable shipbuilding which you and your associates have achieved at Davie Shipbuilding Ltd. over the last decade makes each of you uniquely qualified for the critical production task which faces us on the liquefied natural gas ships we have under contract at Quincy. Because of your record at Davie, we are confident that these ships may be built within the cost, schedule and quality parameters which have been established. We extend to you our full support in your effort to achieve a profitable operation at the Quincy Shipbuilding Division for the successful production of the LNG ships.
>
> We are ready to help you in any way that we can to obtain the necessary work permits/visa.[19]

December 22,1972--The Wall Street Journal reported that Veliotis would replace Lloyd Bergeson as General Manager of the General Dynamics Quincy, Massachusetts shipbuilding yard.[20]

Late December 1972--Veliotis resigned from his position at Davie.

December 27, 1972--In a Defense Department personnel security form, Veliotis said his formal education was as follows:

September 1930 to June 1935, Evagelismos, Piraeus, graduated;

September 1936 to June 1942, St. Paul's College, Piraeus, graduated with a "B. A." degree;

September 1942 to June 1944, Athens University, Athens, graduated with a degree in physics.

May 1944 to May 1947, Royal Naval Academy, Piraeus, graduated with a degree in engineering.

Veliotis said he had a brother, George Eleutherios Veliotis, who lived in New Rochelle, New York. Takis Veliotis gave these references: Joseph G. Gregory, 1019 Maple Avenue, Quebec, whom he had known 20 years; Ross Drouin, 2437 St. Louis Road, Stillery, Quebec, an acquaintance for 20 years; Hazen Hansard, 15 Edgehill Road, Westmount, Montreal, 15 years; Cyrille DeLage, 1165 Delatour, Quebec, 15 years; and Thomas Gibson, 2967 Longfellow, St. Foy, Quebec, 18 years.[21]

December 29, 1972--According to General Dynamics officials, since the Quincy yard was a U. S. government cleared facility, steps had to be taken to obtain required personnel security clearances for Veliotis. The General Dynamics officials said two courses of action were available--first, to apply for a Canadian reciprocal clearance; or, second, to apply for an immigrant alien clearance. According to the GD officials, a Canadian citizen who is in the U. S. under a temporary visa and who has a Canadian top secret or secret clearance may apply for a U. S. secret clearance authorizing access to classified information in connection with the performance of classified work at a facility located in the U. S. A Canadian who has been lawfully admitted to the U. S. under an immigrant visa or permanent visa and who intends to become a U. S. citizen may apply for an immigrant alien clearance. Veliotis decided to apply for both a Canadian reciprocal clearance and an immigrant alien clearance. On December 29, 1972, the appropriate government forms for processing Veliotis's applications were handcarried to the Defense Contract Administration Services Region of the Defense Logistics Agency in Boston.[22]

January 4, 1973--Veliotis formally took charge of the Quincy shipyard. A General Dynamics news release said Veliotis was born in Kariai, Greece.[23] This information was inconsistent with birth data which Veliotis had been giving wherein he informed DOD personnel security officials and Immigration and Naturalization Service officials that he was born in Kranidion, Greece. A World Atlas map of Greece shows Kariai to be many miles from Kranidion. The

GD press release also said Veliotis had earned engineering degrees from the University of Greece and the Laval Technical School in Canada. A Library of Congress report, prepared by the Congressional Research Service at the request of the Subcommittee, suggested that Athens University "may possibly have been called 'the University' or 'the University of Greece' since it was the only university in Greece until 1925, when the University of Thessaloniki was founded."[24, 25] There is no Laval Technical School in Canada. There is Laval University in Quebec. The engineering department of the university has no record of Veliotis having earned a degree there or being enrolled. Laval Institute in Canada is a maximum security prison.[26]

January 4, 1973--Veliotis, now President and General Manager of the Quincy Shipbuilding Division, faced a problem regarding his security clearance. A similar problem affected three of his colleagues at the Quincy facility--Peter J. Gwyn, Assistant General Manager; and Joseph H. Lennox and James H. Gilliland, both Special Assistants to the General Manager. These four men were foreign nationals from Canada. Regulations specifically prohibited disclosure of Naval Nuclear Propulsion Information, both classified and unclassified, to non-U. S. citizens. Because of that prohibition, F. R. Ryan, Manager of Plant Protection at the Quincy yard, notified 12 senior officials of the plant that Veliotis, Gwyn, Lennox and Gilliland "have been notified of their exclusion from access to any and all Department of Defense classified material. Also all KAPL (Knolls Atomic Power Laboratory) and Bettis Atomic Power Laboratory contracts administered for the United States Atomic Energy Commission. This exclusion includes NOFORN, messages, letters and (NNPI) Naval Nuclear Propulsion Information, classified and unclassified."[27]

January 9, 1973--Eight General Dynamics officials met with one DOD representative to "discuss the pros and cons of the facility clearance and the problems involved in facility's possession of nuclear propulsion information, with aliens in top management positions." According to an inter-office memorandum of January 10, 1973 written by Bernard J. Finn, Ralph Gezelman, Acting Chief of Industrial Security in the Boston office of the Defense Logistics Agency, was the government's spokesman at the meeting, which was also attended by Finn, and the following Quincy officials: Domenick Baccari, Manager of the Nuclear Planning and Design Department; Francis R. Ryan, Manager of Plant Protection; and Robert Newell, Facility Security Representative. Representing GD's Electric Boat Division in Groton were William Donegren, Industrial Security Manager; Clayton Prevost, Supervisor of Security and Investigation; and William Pedace, Nuclear Engineering and Design Staff Assistant. Also in attendance was James Budros, Corporate Security Officer at the General Dynamics headquarters in St. Louis. Finn wrote in his memorandum that this group's understanding was that Veliotis and his three Canadian colleagues would apply for permanent status within a month of their arrival at Quincy. Finn went on to say that the group had learned that Veliotis, as a foreigner or as a permanent resident, could not be granted a top secret clearance and that, therefore, the Quincy facility clearance would be downgraded from top secret to "secret Canadian reciprocal," or "final secret clearance," depending on the alien status of Veliotis. According to Finn, Gezelman told the group that:

> ...under present conditions facility clearance would have to be downgraded to secret Canadian reciprocal and that concurrently all government granted top secret and secret personal clearances would automatically be downgraded to secret Canadian reciprocals; also that government granted confidential clearances would be changed to confidential Canadian reciprocal clearances.

However, Finn recounted, William Pedace and William Donegren told the group that Canadian reciprocal facility and personnel clearances would never satisfy the chief of the U. S. Navy's nuclear submarine program, Admiral Hyman Rickover. Pedace and Donegren were quoted to have said that Canadian clearances--

> ...would be worthless, inasmuch as facility possesses Naval Nuclear Propulsion Information (NNPI) and that Admiral Rickover will definitely not permit access to classified and unclassified NNPI by any alien--and in that category he includes foreign nationals and immigrant aliens, cleared or uncleared--in other words, the Admiral has emphatically and consistently stated that only U. S. citizens may have access to classified or unclassified NNPI.[28]

January 10, 1973--The Defense Logistics Agency, responding to the fact that Veliotis and other senior managers at the Quincy facility were immigrant aliens, downgraded the shipyard's facility clearance from top secret to secret. The action was taken in accordance with paragraph 24A(2) of the Industrial Security Manual which stipulated that "an immigrant alien is ineligible for top secret access," and a facility's clearance level "cannot exceed that of the operating officials."[29] Some four years later, in October of 1977, the government took precisely the same action when Veliotis was transferred from Quincy to Groton, Connecticut where he was placed in charge of General Dynamics's Electric Boat Division, which was building the Trident and Los Angeles class nuclear attack submarines for the Navy. The Groton yard, as well as the Quonset Point Facility in North Kingstown, Rhode Island, and cleared employees who worked at these plants, were reduced from top secret to secret clearances. Thirteen months would elapse before Veliotis was given a secret clearance.

January 16, 1973--The presence of Veliotis and his three colleagues at the Quincy yard caused concern at the Department of the Navy. Rear Admiral C. R. Bryan, Deputy Commander of the Naval Shipbuilding Command, wrote to P. G. O'Keefe, Supervisor of Shipbuilding Conversion and Repair, Groton, Connecticut, to say that the Quincy Nuclear Surface Ships Project was under the technical and administrative direction of the Electric Boat Division in Groton. Admiral Bryan went on to point out that sensitive submarine and nuclear propulsion information was housed at the Quincy facility and that the installation under previous contracts had constructed nuclear powered submarines and nuclear submarine support tenders. In addition, the Quincy shipyard had a current contract for nuclear propulsion design work being performed by personnel from the Electric Boat Division in Groton. Admiral Bryan then said:

> NAVSHIPS considers it imperative that immediate action be taken to withdraw or appropriately isolate all submarine and naval propulsion information held at the Quincy shipyard so that access by foreign national management will not be possible. While all currently active nuclear propulsion work is under the cognizance of Electric Boat, it is not clear that satisfactory security arrangements exist since the Quincy Shipbuilding Division still provides administrative and security support services.[30]

February 13, 1973--Responding to Admiral Bryan, J. F. Burns, Director of Nuclear Engineering at the Electric Boat Division, wrote to spell out General Dynamics's intention to adhere to security requirements at the Quincy facility, including its procedures calling for "exclusion of non-U. S. citizens." General Dynamics, Burns said, would adhere to Navy regulations on "safeguarding of naval nuclear propulsion information and complying with NOFORN security requirements at Quincy." In that regard, Burns wrote, "all employees without security clearances have distinctive colored identification picture badges. Personnel wearing this type of badge are excluded from Nuclear Project and controlled access areas." Burns attached to his memorandum "written acknowledgements," or affidavits, "on the part of new management members that access to certain areas of the plant are prohibited by their lack of clearance."[31]

February 16, 1973--Colonel Donald T. Clark, Chief of the Office of Industrial Security in the Defense Supply Agency Headquarters at Cameron Station, Virginia, discussed personnel security problems caused by the Veliotis appointment in a memorandum to Defense Logistics Agency officials in Boston. Not only was Veliotis's presence at the Quincy yard a problem, but also the new General Dynamics officer was causing difficulties for the firm's corporate activities in St. Louis. Currently enjoying a top secret facility clearance, the General Dynamics Corporation itself would have to be downgraded to the secret level because Veliotis, in addition to running the Quincy plant, had also been named a Corporate Vice President. Colonel Clark said any request to exempt General Dynamics from this dilemma "would have to be considered at the DOD level." The issue of General Dynamics's corporate security clearance level was never raised again in any of the documents seen by the Subcommittee staff.[32]

February 21, 1973--P. G. O'Keefe, Supervisor of Shipbuilding Conversion and Repair at Groton, personally inspected the Quincy yard. In a memorandum to the Naval Ship Systems Command, O'Keefe reported that security procedures regarding Naval Nuclear Propulsion Information at the Quincy facility were adequate to prevent "intentional counter-pressure /from being/exerted by top management;" that is, by Veliotis, Gwyn, Lennox and Gilliland. However, O'Keefe wrote, it would still be "desirable and appropriate" to post pictures of the four men at all entrances to areas containing Naval nuclear propulsion data "to preclude inadvertent access to the four foreign nationals."[33]

February 26, 1973--D. G. Gigizas, the Mayor of Kranidion, Greece, signed a notarized statement in which he certified to these facts regarding Veliotis's birth:

> Panagiotis Veliotis, from Kranidion, Ermiondos County, son of Eleftherios and Ionna, was born in Kranidion, is registered in our Town Registry for males no. 45, year of birth 1926, Greek nationality by birth, registration no. 2564/2-21-73 by order of the Prefecture of Argolidos.
>
> This certificate is issued for all legal purposes.

The Mayor's certification was written in Greek and translated by the Berlitz Translation Service of Boston.[34] It is not apparent from the Mayor's declaration who requested it, or what use was made of it. The Subcommittee obtained a photostat of it from General Dynamics.

March 23, 1973--A memorandum from Gorden E. MacDonald, a corporate Vice President of General Dynamics, to company Chairman David Lewis indicated that questions had been raised about the manner in which Veliotis and his management team, now in control of Quincy Shipbuilding, had run Davie Shipbuilding. MacDonald had spoken with a senior Canadian business executive who had on October 26, 1972 recommended Veliotis for the Quincy job. The Canadian executive now was telling MacDonald that his "opinion of Mr. Veliotis was unchanged" and that recently publicized questions about Davie management under Veliotis had not weakened his confidence in Veliotis's "integrity or his ability." MacDonald added, though, that the senior Canadian business executive cautioned him:

> ...this does not mean that the General Dynamics Corporation should not keep a close eye on this new group to be satisfied before really turning them loose to operate that particular division. This is a safeguard that all corporations implement on any new hire in a key spot.

According to the MacDonald memorandum, the questions were raised in a Wall Street Journal article.[35] At the Subcommittee's request, the Library of Congress conducted a search for such an article but the search was unsuccessful.

May 18, 1973--Veliotis submitted information to the Defense Department for a National Agency Check, or NAC, wherein the government tries to obtain pertinent information on file on a person in the FBI and other federal agencies. In this document, Veliotis said he was born on August 11, 1926. He said that he began his employment with Davie Shipbuilding of Quebec in 1953. He said that his father, Eleutherios Veliotis, a Greek citizen, was dead; and his mother, 79-year-old Joanna Zarifis Veliotis, a Canadian citizen born in Kilas, Greece, lived at 2410 St. Louis Road, Quebec City, with his wife and children. Under the question, "Has the subject had employment requiring a security clearance or investigation?" Veliotis had answered yes. In a typed notation, it was asserted that the clearance was "secret Canadian" but also noted was the fact that "no record in DISCO," which seemed to indicate that no record of the secret Canadian clearance was contained in the files of the Defense Investigative Service or the Defense Industrial Security Clearance Office in Columbus, Ohio. The NAC, or National Agency Check, request was stamped "expedite" and "immediate action."[36] At the Subcommittee's request, DIS has tried to confirm that Veliotis actually had a Canadian reciprocal secret clearance for the one year during which he was in charge of the Quincy shipyard with its military and nuclear propulsion programs. No such confirmation has been turned over to the Subcommittee.

June 7, 1973--Defense Investigative Service Special Agent R. W. Magill of the South Weymouth, Massachusetts office reported on the progress being made on the Veliotis personnel security inquiry. Under the heading of "Birth," Magill said, "Subject's date and place of birth confirmed from employment records." It is not apparent which employment records--were they from Davie Shipbuilding of Quebec or General Dynamics of Quincy?--nor is it apparent from this report what records Magill actually saw. It is informative to recount, for example, that whatever records of birth were available in 1973 were considered insufficient by someone because, as noted above, verification of Veliotis's facts of birth was sought from and provided by D. G. Gigizas, who identified himself as the Mayor of Kranidion, Greece, but the Mayor did not provide copies of a birth certificate or any other documentation; nor did he give the exact date of birth, except to confirm that Veliotis was born in 1926. Special Agent Magill's efforts to vet Veliotis were made more difficult when the Commonwealth of Massachusetts, Veliotis's place of residence since his arrival in the U. S. about six months earlier, refused to cooperate with federal authorities. As noted by Magill, "A check of Quincy, MA, Police Department records could not be conducted since the Massachusetts Criminal History Systems Board has issued a preliminary ruling that the laws of the Commonwealth of Massachusetts prohibit the release of information in such records to the Department of Defense for personnel security purposes."[37]

June 8, 1973--DIS files reflect the stamped declaration that "DIS NAC Center NAC completed favorably per DOD Dir. 5210.8." It was signed L. F. Flynn.[38]

June 13, 1973--Veliotis applied for permanent residence status in the United States. Patrick Toomey, Director of the Boston office of the Immigration and Naturalization Service, informed Veliotis that his request had been granted.[39]

1973--Veliotis and his Special Assistant, James Gilliland, were involved in the award of a $44 million subcontract to Frigitemp Corporation of Brooklyn, New York, a shipfitting and insulation concern. The contract was in connection with construction of five huge cryogenic tanks designed to carry liquefied gas at temperatures close to absolute zero. It would later be charged by a federal grand jury in New York that Veliotis and Gilliland received a $2.7 million kickback in exchange for awarding the contract to Frigitemp.[40]

July 12, 1973--DIS Special Agent L. D. Gianascol of the Boston office filed a report of investigation on Veliotis's personnel security inquiry preparatory to Veliotis's obtaining a secret clearance needed for his position as President - General Manager of the Quincy yard. It is not apparent from available records what clearance Veliotis was working under at the time because he assumed the top job at Quincy on January 4, 1973 and, as will be noted below, did not receive a secret clearance until January 23, 1974. In any event, Special Agent Gianascol reported that he had developed no derogatory information on Veliotis. Devoting considerable attention to Veliotis's 1969 divorce from his first wife, Gianascol went on to note one "variance" -- the fact that Panagiotis Takis Veliotis also had used the name Panagiotis Eletherton Veliotis.41

July 16, 1973--DIS Special Agent B. J. Haupt of the South Weymouth office reported on remarks Veliotis had made to him in a sworn statement, the full text of which follows:

Q. Do you intend to reside permanently in the United States?

A. Yes.

Q. Do you intend to acquire United States citizenship?

A. Yes. I intend to become a citizen of the United States as soon as I become eligible.

Q. Do you own any stocks or bonds issued by a foreign company or government?

A. No.

Q. Do you own or have an interest in any land or buildings located outside the United States?

A. Yes, at the present time I own a home in Quebec, Canada, which is for sale.

Q. Would you lose your home if you became a citizen of the United States?

A. No.

Q. Could your home be arbitrarily confiscated by any authority?

A. No.

Q. To which country do you owe primary allegiance?

A. I owe primary allegiance to the United States.

Q. What is your general attitude toward the United States vis-a-vis the country of your present citizenship?

A. The United States offers a far greater future, education is greater and there is more freedom in the United States.

Q. Do you have a military obligation to a foreign country?

A. No.

Q. What are your reasons for being in the United States?

A. The United States offers a challenge to me, far greater educational opportunity for my children and a better future for myself and my family.

Q. Do you hold any retirement rights in a foreign government or company?

A. No.[42]

July 27, 1973--DIS Special Agent A. J. Pfeiffer of the St. Louis office reported on his interview with Gorden E. MacDonald regarding Veliotis. MacDonald, Executive Vice President of General Dynamics, said he had "weekly to monthly contact as a work associate" of Veliotis going back to November of 1972, Pfeiffer wrote, pointing out that MacDonald "provided only favorable information about Veliotis" and recommended him for a top level assignment. Special Agent Pfeiffer also sought to interview Hillyard Paige, Corporate President of the St. Louis-based General Dynamics, Veliotis's boss, but Paige was out of town.[43]

August 9, 1973-- Special Agent Jonathan D. Makris, apparently with the USAF office of Special Investigations, reported on his inability to confirm two key assertions Veliotis had made about his past. Veliotis had written on his DOD personnel security questionnaire of December 27, 1972 that he had attended the Athens University from September of 1942 to April of 1944 and had graduated with a degree in physics. Panagiotis Tassopoulos, Secretary of the School of Physics at Athens University, informed Agent Makris that he could not locate any of Veliotis's records because the period of time when Veliotis reportedly was a student occurred during the German occupation "and that the school records are incomplete during that period." Veliotis's reported military career was also unverifiable. Agent Makris reported that the Greek military authorities had "advised that the dates of subject's service, branch, serial number and where served, is needed to verify subject's service."[44]

August 30, 1973--DIS Special Agent F. P. Boyda of the office in Waltham, Massachusetts reported that Hanson S. Reynolds of 14 Colchester Street in Weston, Massachusetts provided only favorable information about Veliotis and recommended him for a position of trust. Reynolds, Veliotis's attorney, said he had met with his client twice a month since January.[45]

August 31, 1973--DIS Special Agent Magill of the South Weymouth office reported that Kenneth D. Hanson of 1 Acorn Lane, Marshfield, Massachusetts had been interviewed as a reference for Veliotis. A bank vice president, Hanson said he had known Veliotis and had monthly contacts with him as a "business associate" since the previous January and offered no derogatory information about him and recommended him for an important post, Magill wrote.[46]

September 7, 1973--Special Agent K. R. Doktor of the DIS office in New York City reported on an interview about Veliotis with Kimon Petzos, Vice President of Arvan Ltd., located at 1 Rockefeller Plaza. Giving only favorable information, Petzos said he had been a friend of Veliotis since 1953 and saw him four times a year.[47]

September 8, 1973--Veliotis travelled to Russia on business. He returned to the U. S. on September 12, 1973. It was one of 13 trips out of the U. S. Veliotis took in 1973. Other foreign trips that year included nine pleasure trips to Canada, one pleasure trip to Greece, and two business trips to Japan.[48] The Industrial Security Manual requires that a person with a secret clearance or above must report travel to a Communist country. DIS has been unable to find any evidence that Veliotis's trip to Russia was reported. DIS officials have advised that, while the report of such a trip is required following the journey under the current rules, the 1973 regulations called for advance and post-notification of such a visit. Specifically, paragraph 6 b. 9 says:

> The contractor shall submit a report...on completion of travel to or through a Communist country, or attendance at an international meeting where Communist representatives participated or attended. The report shall include the employee's full name, clearance status, date and place of birth, a brief description of the projects, including the category of classified information, to which he or she had access during the past two years...the countries visited or the meeting attended, the dates of the travel, and the employee's statement of the purpose and objective of the travel. The report shall include, if appropriate, a narrative statement of the circumstances surrounding all hostile intelligence efforts to obtain information from or to compromise the traveler, or any endeavor by an unfriendly interest to establish a continuing relationship with the employee.[49]

September 17, 1973--Special Agent P. C. Miller of the Milwaukee office of DIS reported on his interview with Charles Lee Spees, who offered no derogatory information about Veliotis and recommended him highly. Lee, who gave his address as P. O. Box 164, Elkhorn, Wisconsin, said he was retired now but that from 1955 to 1965 he had had weekly contact with Veliotis on business matters and had "yearly" contact with him on a social basis from 1965 to 1973. "Spees remarked that he firmly believed that subject will become a U. S. citizen when subject becomes eligible for citizenship," Miller wrote. It is informative to note that of the seven persons interviewed as references for Veliotis, not one of them reported having known him prior to 1953.[50]

January 23, 1974--The Defense Industrial Security Clearance Office (DISCO), located in Columbus, Ohio, advised the Quincy yard that a secret clearance had been granted Veliotis.[51]

January 24, 1974--J. L. Budros, Corporate Director of Security for General Dynamics, sent a memorandum to Algie A. Hendrix, Vice President for Industrial Relations of the firm, to note that Veliotis and Peter Gwyn both had secret clearances and that two other Canadians at Quincy--Joseph Lennox and James Gilliland--were carrying "Canadian reciprocal secret" clearances. Budros said Lennox and Gilliland had access to secret level information and added that, "Of course, as Foreign nationals all of the four men will continue to be ineligible for access to Naval Nuclear Propulsion Information and related submarine technology--classified or unclassified."[52]

October 22, 1975--Veliotis's new clearance proved to be problematical, however, at least in connection with the Naval Nuclear Propulsion Information work being conducted at Quincy. On October 22, 1975, Warren G. Sullivan, Vice President for Industrial Relations at General Dynamics headquarters in St. Louis, wrote to Vice Admiral Robert C. Gooding, Commander of the Naval Sea Systems Command, to request a "waiver of requirements for access to classified and unclassified naval nuclear propulsion information by a foreign national." Pointing out that the Quincy yard was preparing a proposal for the design and construction of a nuclear strike cruiser, known as CSGN, Sullivan said it was "essential" for Veliotis to have access to certain classified information in his capacity as General Manager.[53]

November-December 1975--Admiral Gooding granted the waiver in a November 14, 1975 letter to Sullivan. He said Veliotis would be required to sign an affidavit setting forth his knowledge of the terms of the waiver and his avowal to require access only to that nuclear propulsion information necessary for the development of the General Dynamics design and construction proposal.[54] Veliotis signed the affidavit on November 24, 1975. Sullivan, writing Admiral Gooding on December 3, 1975, asserted that D. M. Baccari, the Quincy Manager of the Nuclear Surface Ships Project, and Spencer Reitz, the Shipbuilding Division Project Manager, would be responsible for seeing to it that all security requirements would be met in executing the waiver affecting Veliotis.[55]

December 1975--General Dynamics issued a biographical sketch, in press release form, on Veliotis, saying about his formal education and military record that he "earned degrees at St. Paul College, Royal Naval College and the National University, Athens, Greece. During World War II he served in the Middle East with the Royal Hellenic Navy."[56]

February 3, 1976--Alfred E. Dupell, Director of the Security Division in the Naval Sea Systems Command, advised Quincy officials that the special security procedures for carrying out the Veliotis waiver were acceptable and hereby approved.[57]

December 1, 1976--General Dynamics filed $544 million claim against the Navy in connection with SSN 688 cost overruns.[58]

March 20, 1977--Veliotis travelled to Algeria and returned to the U. S. on March 24, 1977. It was one of 31 foreign trips he made from 1974 through March of 1977, including four business trips to Switzerland, 12 pleasure trips to Canada, four business trips to England, three business trips to Indonesia, two pleasure trips to Greece, two business trips to Japan, and single business trips to Belgium and the Netherlands, Japan and Indonesia, and Portugal.[59]

July 19, 1977--General Dynamics was already planning the promotion of Veliotis from the Quincy shipyard to the Electric Boat Division in Groton, Connecticut. Personnel security concerns stemming from Veliotis's immigrant alien status still posed a problem for the firm and these problems were addressed--and solutions to them put forward--in a memorandum written at the corporate level by C. J. (Chuck) Middleton. Noting that Veliotis had a secret clearance as well as a Navy-approved waiver permitting him limited access to naval nuclear propulsion information for work on the nuclear strike cruiser proposal at Quincy, Middleton said Gorden MacDonald, currently manager at Electric Boat, held, as did his predecessor, a Mr. Pierce, a top secret clearance from DOD and a "Q" access authorization from the Energy Department. These clearances were in line with the Industrial Security Manual requirement that the management official in charge of a facility had to be cleared at the same level as the plant clearance. At this time, Veliotis could not qualify for a top secret clearance because immigrant aliens were prohibited from such designation, Middleton said, adding:

> Several defense contractors have petitioned DOD for a waiver to this requirement in the past and all have been denied...by the Assistant Secretary of Defense (Comptroller) Fred P. Wacker.

Veliotis was not only ineligible for a top secret clearance, Middleton said, he was also precluded from working on Energy Department nuclear programs because he lacked a "Q" access authorization. Both the top secret and the "Q" would be required at Electric Boat, Middleton said. But there was a solution to this problem, Middleton said, explaining that Veliotis could be given a top secret and a "Q" access upon his naturalization as a U. S. citizen, an opportunity available to him at the completion of a five-year residency requirement on June 13, 1978. Middleton said the five-year residency requirement for citizenship might be shortened for Veliotis "through special legislative action." But apparently the firm did not want to wait one year or less to install Veliotis at Groton so General Dynamics officials chose the second solution offered by Middleton. That was to bring Veliotis on as General Manager of Electric Boat with the understanding that the Pentagon would downgrade the entire Groton facility and its sister site at Quonset Point, Rhode Island, from top secret to secret just as DOD officials had done at Quincy when Veliotis took charge there four years earlier. Middleton described this solution this way:

> Downgrade the EB facility clearance to secret level. Although EB has a top secret clearance, it is infrequently needed for engineering study or support work. We could investigate the possibility of whether one of the engineering buildings at EB could have a separate facility clearance at top secret for this type of work and then lower the clearance to secret for the rest of the facility. I have been advised that EB has no top secret classified material or information presently on hand. If their top secret work is done off site, then the persons involved could be granted top secret clearances as Type A consultants by the Navy or other agency.
>
> If the facility clearance can be lowered, then Mr. Veliotis' current secret clearance would suffice. However, we would still need to get Navy approval to grant him access to NNPI. Also we would still need to get a clearance from ERDA to cover his responsibilities for SBG site.

Middleton said Veliotis's control over the Quonset Point facility was not a problem because, while the installation did have a top secret clearance, no top secret or nuclear work was performed there. Middleton added that he was preparing a letter requesting a "Q" access authorization for Veliotis.[60] That letter, signed by GD Chairman David Lewis, went out to the Naval Sea Systems Command and the Energy Department, dated July 22, 1977.[61]

July 25, 1977--Arch H. Rambeau, Director of Personnel and Management Relations for General Dynamics, wrote a memorandum regarding, "Personnel Activities Preceding Selection of New General Manager for the Electric Boat Division." Pointing out that the two most senior management officers at the Groton facility had retired, Rambeau said Electric Boat had enlisted two executive search companies--the Kennedy Group of Westport, Connecticut and Dressel, Dimmitt and Andrews of Chicago--to locate qualified candidates for the position of General Manager. More than 50 persons were considered for the post, Rambeau said, adding that after "months of careful review and screening" of candidates, it was decided that no American citizen was qualified and that "the best available" choice was P. Takis Veliotis, President and General Manager of GD's Quincy yard. "After all of the extensive efforts, it has been concluded that there is no individual as fully qualified to manage the Electric Boat Division as P. Takis Veliotis," Rambeau concluded. The business executives considered in the executive search, Rambeau said, included L. C. Ackerman of Newport News, Mac C. Adams of Avco Corporation, Ralph Anselmi of Todd Shipyards, George R. Armstrong of U. S. Caterpillar Corp., George Arnold of Armco Steel, John Banks of National Steel Shipbuilding, Robert W. Boeke of John Deere & Co., Albert Bossler of Avondale Shipbuilding, Leo P. Brewer of Cummings Engine, William Brigham of Bethlehem Steel, Eugene J. Cattabiani of Westinghouse Electric, Tom Cleary of Lykes Youngstown Steel, William H. Collins of Bethlehem Steel, J. O. Crooke of Bethlehem Steel, H. C. Ewing, Jr., of Newport News Shipbuilding, Marty Ingwerson of Lockheed Shipbuilding, W. Gordon Jarvis of Combustion Power Corp., Max T. Johnston of Westinghouse Electric Corp., James B. Kelly of Combustion Engineering, John Kopp of American Shipbuilding, Robert S. Leventhal of Engelhard Minerals-Chemical Corp., Joseph Lieb of Maryland Shipbuilding & Dry Dock, Douglas J. Logan of Otis Elevator, James A. Maggetti of Kaiser Steel, Richard A. Mayr of American Shipbuilding Co., Keith Mazurek of International Harvester, Donald E. Peterson of Ford Motor Co., Pat Phillips of Newport News Shipbuilding, John D. Reilly of Todd Shipyards, Marvin T. Runyan of Ford Motor Co., Farrell S. Sanders of Newport News Shipbuilding, John J. Slack of Combustion Engineering, Larry W. Todd of Rockwell, Rear Admiral Tom Westfall, USN, Walter Williams of Bethlehem Steel, Graham Wipple of Lockheed Shipbuilding and A. P. Zechella of Westinghouse Electric Corp.[62]

July 25, 1977--David S. Lewis, Chairman and Chief Executive Officer of General Dynamics, sent a letter to Vice Admiral C. R. Bryan, Commander of the Naval Sea Systems Command, to request a "Q" access designation for Veliotis. The expanded access was necessary, Lewis said, because General Dynamics planned to transfer Veliotis from Quincy to Groton where Trident submarines were being built. Lewis described Veliotis's background, his proven ability as a competent and innovative shipbuilding executive and a resident alien from Canada who would soon be eligible for American citizenship. Lewis said:

> ...Takis Veliotis has very unusual talents and skills not possessed to a comparable degree by an available United States citizen, known to us, and the position for which he is considered is one that is essential to the furtherance of the AEC's [Atomic Energy Commission] program. Accordingly, we request your assistance and approval in authorizing the processing of Takis Veliotis's application for "Q" access which when approved will permit him to become the general manager of the company's Electric Boat Division.

Lewis sent a similar letter on July 26, 1977 to H. E. Lyon, Director of the Division of Safeguards and Security in the Energy Department. About Veliotis's past in Greece, Lewis wrote that Veliotis was born in Kranidion, Greece, attended the Greek Royal Naval Academy from 1944 to 1947 and worked for his father as a marine engineer from 1947 to 1953 when he emigrated to Canada, became a Canadian citizen and went on to become President and General Manager of Davie Shipbuilding.[63]

June 28, 1977--Veliotis signed an Energy Department personnel security questionnaire in which he noted that he had never been arrested, charged or held in connection with a criminal offense.[64] Both the FBI and the Energy Department would have seen this questionnaire and would also have seen the FBI file indicating the June 7, 1954 conviction in Piraeus.

August 2, 1977--Admiral H. G. Rickover, Director of Naval Reactors, wrote H. E. Lyon at the Energy Department to request a "Q" access designation for Veliotis. Rickover said established Energy Department procedures regarding "access authorization for aliens" had been satisfied in the Veliotis matter. Rickover also noted General Dynamics's "unsuccessful efforts to find a U. S. citizen for this position who is available and acceptable" as evidence of the necessity to give the job to Veliotis and to grant him the needed access.[65]

August 5, 1977--William H. Walsh, Director of the Division of Safeguards and Security at the Schenectady Naval Reactors Office, wrote the FBI to request a full field investigation of Veliotis. This inquiry was in response to the request to give Veliotis an Energy Department "Q" access authorization.[66]

August-October 1977--Veliotis remained at Quincy with his secret clearance and his special waiver exempting him from the foreign national exclusion for 20 months. Then in response to the requests to give Veliotis a "Q" access designation, an investigation was conducted by the Federal Bureau of Investigation. Provided with the results of that FBI inquiry, the Energy Department approved the request. According to a memorandum of October 13, 1977 to Admiral Rickover from H. E. Lyon, the "Q" access had been bestowed on Veliotis.[67] B. F. Erickson, Manager of the Energy Research and Development Administration's Schenectady, New York Naval Reactor Office, wrote General Dynamics on October 19, 1977 to say that Veliotis had a "Q" access clearance and an Energy Department file number, SC S9111 WA, and that this clearance was to be withdrawn when Veliotis's need for such sensitive data no longer existed.[68]

September 27, 1977--An Energy Department "summary statement," used in adjudicating Veliotis's application for "Q" access, noted that two of his character witnesses--Lewis H. Weinstein of Waban, Massachusetts and C. Lee Spees of Elkhorn, Wisconsin--recommended that the expanded clearance be given. "...outstanding man who values principles of American democracy," said Weinstein, whose endorsement was seconded by Spees, who said Veliotis was "loyal to U. S. in all matters." The Central Intelligence Agency was reported to have no information on Veliotis but the FBI had learned that 23 years earlier--on June 7, 1954--Veliotis had been sentenced to 45 days in jail in Piraeus for money order fraud. No other derogatory information was stated.[69] As noted earlier in this chronology, there is an inconsistency in the FBI's sentencing date and Veliotis's reported arrival in Canada. The Bureau said Veliotis was sentenced on June 7, 1954. In his biographical data, Veliotis wrote that he arrived in Canada in 1953 when he went to work for Davie Shipbuilding in Quebec. Senator Nunn asked the FBI for the investigative files on the Veliotis background inquiry regarding the "Q" access request. On March 26, 1985, the Justice Department informed the Subcommittee Minority staff orally that Senator Nunn's request for the 1977 file had been denied. A written confirmation of this denial would follow, the Department said.

September 29, 1977--An Energy Department "file summary sheet" of this date contained a handwritten notation that Veliotis's "arrest 25 years ago not listed" but the summary sheet provided no further information on this point. This document also noted that the FBI had completed its full field investigation on September 27, 1977.[70]

October 21, 1977--On this date, two days after his formal notification of the "Q" access designation, Veliotis was reassigned, being named a Corporate Vice President and General Manager of the Electric Boat Division with full responsibility over operations at Groton and the Quonset Point Facility in North Kingstown, Rhode Island, as well as off-site locations. Announcement of the action was made by David S. Lewis, Chairman of General Dynamics, who also noted that in his new job Veliotis would be reporting to him. Other personnel actions affecting the Veliotis management group announced by Lewis included the selection of Peter J. Gwyn as Acting General Manager of the Quincy Division; and James H. Gilliland who would "take the responsibility for insuring that our on-going new ship sales activities would continue without interruption. New orders are vital to the long term health of the Quincy Division and no opportunity for a profitable sale can be missed."[71] General Dynamics officials have sought to convey the idea that, as he looked back upon his nearly five-year stint at the Quincy yard, Veliotis could point to a job well done. GD Chairman Lewis said the work on the Burmah Oil LNG tanker contract was performed competently and resulted in profits for the firm. Veliotis "did a good job for the company the whole time he was there. We made money on the shipyard," Lewis was quoted by Forbes as having said. But the magazine reported a contrary view held by other executives, when it recounted:

> Several high ranking officials from the Burmah side--those most familiar with the tanker business--say the ships were so badly built under Veliotis that major reworking was done in Japan. Maintenance was costing several million per year per ship, about triple GD's original estimates. These officials believe that construction overcharges may have been in the $100 million area....[72]

October 28, 1977--The transfer of Veliotis to head both the Groton and Quonset Point facilities caused the armed services to make adjustments regarding personnel security. On October 28, 1977--a week after Veliotis's new assignment was announced--the Defense Logistics Agency wrote him. In a letter from R. E. Nehls, the agency's Director of Industrial Security, Veliotis was advised that because of the status of his own security clearance, it was necessary to downgrade the clearance of both the Groton and the Quonset Point facilities from top secret to secret but that this action was being taken "without prejudice" and was not to be interpreted as a disciplinary sanction against him. The action, which also downgraded the clearance levels of all employees at the facilities, was being executed, Nehls said, according to paragraph 24a(2) of the Industrial Security Manual which stipulated that "an immigrant alien is ineligible for top secret access," and a facility's clearance level "cannot exceed that of the operating officials."[73]

December 5, 1977--Vincent M. Pusateri, Chief of the Personnel Security Branch of the Energy Department's Security and Safeguards Division, wrote a memorandum to the Division Internal Security Branch Chief, M. J. Dowd. "Report on granting of 'Q' access authorization to alien" was the subject of the Pusateri memorandum, which was written to satisfy the Department regulation requiring that the granting of a security clearance had to be duly recorded, along with pertinent information about the alien, including date and place of birth, Social Security number, dates and status of immigrant status and descriptions of his job and access to secured areas and information. Pusateri wrote that Veliotis's clearance was sponsored by Admiral Rickover, chief of the Navy nuclear propulsion program, and authorized by retired Admiral Harvey E. Lyon, head of the Department's clearance adjudication office.[74]

Late 1977--Faced with serious management and labor problems at the Groton facility, Veliotis laid off about 3,000 employees to reduce overhead costs. Work tasks for the remaining 20,000 workers were revised over the next several months. Veliotis also began pressing for the General Dynamics insurance claim regarding the SSN 688 program.[75]

February 1978--IDT Corporation was formed by former officials of Frigitemp, whose financial position had deteriorated.[76]

March 1978--Frigitemp filed for bankruptcy. Lawson F. Bernstein was named bankruptcy trustee.[77]

June 9, 1978--General Dynamics was now claiming to have suffered losses of $718 million in the SSN 688 attack submarine contract, losses that the company claimed were not its fault. The Navy settled for $359 million.[78]

February 1979--A federal grand jury was convened in Hartford to examine allegations that Electric Boat and General Dynamics had filed fraudulent claims regarding the SSN 688 cost overruns. Impetus for the grand jury inquiry was provided, in part, by Admiral Rickover, who had been a critic of General Dynamics regarding the SSN 688 contract overruns. Rickover said Electric Boat was charging considerably more for SSN 688 construction than was the Newport News Shipbuilding and Dry Dock Company for the same vessel.[79]

March 28, 1979--Veliotis became a naturalized American citizen. His certificate of naturalization number was 10314947.[80]

January 1980--J. W. Rannenberg, Director of Contracts at the Groton yard, wrote the Navy to say that testing requirements under a Trident submarine construction contract made it vital that the Groton facility's clearance be upgraded from secret to top secret.[81]

February 8, 1980--General Dynamics promoted Veliotis to the newly created position of Executive Vice President. This assignment gave Veliotis control over the Quincy and Groton shipyards and off-sites. In a press release on this promotion, General Dynamics quoted Chairman Davis Lewis who said the "appointment is highly deserved," a reflection of the company's confidence in Veliotis's management skills. In a brief biographical reference in the press release, General Dynamics provided this information about Veliotis's pre-1953 career:

> During World War II, he served as an officer in the Royal Hellenic Navy and was decorated for his wartime service by the late King Paul and Queen Frederika.[82]

February 14, 1980--The Navy asked the Defense Logistics Agency to reinstitute the top secret clearance for the Groton shipyard.[83]

February 1980--Frigitemp bankruptcy trustee Lawson Bernstein conducted depositions of Veliotis and Gilliland. Lawyers for General Dynamics attended the depositions.[84]

March 4, 1980--Patricia A. Hill, Contracting Officer for Security Matters in the Naval Sea Systems Command, endorsed the idea of reinstating the top secret facility clearance for the Groton shipyard. In a memorandum to Defense Logistics Agency officials in Boston, Hill said the higher clearance should be reinstated as soon as possible so that Electric Boat could carry out its work on the Trident submarine contract.[85]

March 12, 1980--Wesley W. Parke, Chief of the Technical Support Division of the Directorate of Industrial Security of the Defense Logistics Agency, wrote F. R. Ryan, General Dynamics's Security Director at the Groton yard, to advise him that the request for a top secret clearance for the Groton facility had been approved.[86] That same day--March 12, 1980--the Defense Industrial Security Clearance Office gave Veliotis a top secret clearance.[87] DIS, which turned over to the Subcommittee its files on the 1973 personnel security inquiry regarding Veliotis's secret clearance, had no files on the 1980 top secret clearance. This suggested the possibility that no background check was conducted on Veliotis for the top secret clearance; and that the Defense Industrial Security Clearance Office, adjudicator for defense contractor employees, had no timely information upon which to base its decision to give Veliotis the higher clearance. According to the Industrial Security Regulation of February 1984 (DOD 5220.22-R), a duly-authorized "Q" access authorization from the Energy Department "is considered an authoritative basis for a DOD clearance at the top secret level." That is to say, DOD will accept the "Q" designation as sufficient evidence to justify waiving the need for subjecting the candidate for top secret clearance to the normal vetting procedures. There are, however, specific paperwork requirements in this process such as the submission by the candidate or his employer of a DD Form 48-3 to the Defense Industrial Security Clearance Office. In addition, DISCO must obtain verification of the "Q" clearance, the date the investigation was completed, the name of the investigative agency and case file number and a statement from the Energy Department that no derogatory information has been developed since the clearance was granted. DIS said it adhered to all established procedures in granting Veliotis a top secret clearance based on the Energy Department "Q" access authorization.[88] It should be noted that there were two pieces of derogatory information in the Energy Department's "Q" investigation conducted by the FBI. First, there was the reported June 1954 conviction of Veliotis in Piraeus for reported money order fraud and his 45-day jail sentence. Second, there was the unreported trip Veliotis made in September of 1973 to a Communist nation, Russia. Neither of these alleged "derogatories" had been resolved by the Energy Department prior to Veliotis's having been given the "Q" authorization by the Department. Similarly, the apparent inconsistency of dates--Veliotis's assertion that he arrived in Canada in 1953 contrasted with the report of the 1954 conviction in Piraeus--does not appear to have been resolved. Procedures for waiving investigation on a "Q"-cleared candidate for top secret are spelled out in ISR 2-309; p. 105.

May 1, 1980--Veliotis was promoted to serve on the General Dynamics board, but continued to manage the Groton shipyard.[89]

September 15, 1980--F. R. Ryan, Director of Security for the Electric Boat Division in Groton, said that not only did his shipyard require a return of its top secret clearance, but so also did the Quincy facility. Electric Boat intended to utilize the Quincy yard on the Trident contract, Ryan said in a letter to the Defense Logistics Agency in Boston. Ryan warned:

> If the Quincy Shipbuilding Division fails to obtain a top secret facility clearance, it would have significant impact on the Electric Boat Division as well as the Marine Operations of General Dynamics Corporation.[90]

September 29, 1980--The Defense Logistics Agency reinstated the Quincy yard's top secret facility clearance.[91]

1981--The Navy tried to persuade General Dynamics to remove Veliotis from control of the Groton yard. Navy Secretary John Lehman acknowledged his Department's move against Veliotis when he said, "We insisted...that before they got another contract they commit to get him out of Electric Boat. We didn't trust him....We felt he was a poor manager and that he was constantly picking fights with the Navy and the yard."[92]

October 5, 1981--General Dynamics issued a press release to respond to news reports "speculating on management assignments at the company's Electric Boat Division." Chairman David Lewis was quoted saying:

> Mr. Veliotis continues to be a valued senior executive of our company. At the right time during the next several months, we expect he will be given additional responsibilities of major importance to the long term future of General Dynamics. These moves will be made in a manner and on a schedule whose primary consideration will be the best interests of the Navy submarines under contract at Electric Boat.[93]

November 1, 1981--Veliotis was named Executive Vice President for Marine and International Operations.[94]

December 1981--The federal grand jury in Hartford concluded its investigation. No charges were brought.[95]

December 31, 1981--Veliotis's year end base salary combined with incentive compensation in 1981--the last full year he was employed at General Dynamics--was $310,000. Previous year end base salaries with incentive compensation were $280,000 (1980), $223,000 (1979), $192,000 (1978), $175,000 (1977), $150,000 (1976), $138,000 (1975), $116,000 (1974), and $100,000 (1973). In addition, in that nine-year period, Veliotis was awarded options on 73,656 shares of stock.[96] His salary and raises are included here to underline the question of whether or not Veliotis was displaying a level of living beyond his income, another possible indicator of potential wrongdoing that a more effective personnel security program might have picked up. Sudden or unusual signs of affluence are common signals personnel security specialists are trained to look for in suspected employees, no matter what their rank. Veliotis seemed to stand out because of the generous manner in which he supported himself. Joe Williams, Jr., a retired Naval officer who left the service of Admiral Rickover and went to work for Veliotis at Electric Boat, was quoted in Forbes as saying, "I got the impression there was money in the family." The magazine, noting Veliotis's "20-room mansion in Massachusetts," his "waterside condo in Florida" and his yacht Paulene II, recounted that his "associates only remember that he always acted as if he had money."[97] One senior General Dynamics official, himself apparently well compensated for his services, said that he had worked with Veliotis on occasion and had been struck with the question of how Veliotis could live as well as he did on what he made.[98]

December 31, 1981--According to information provided the Subcommittee by General Dynamics officials, David Denton, Assistant U. S. Attorney in the Southern District of New York, wrote Veliotis to request his voluntary appearance before the grand jury investigating the alleged Frigitemp kickback scheme.[99]

January 25 and 26, 1982--These are the dates on subpoenas served by the federal grand jury compelling Veliotis to testify and General Dynamics to turn over certain records in the alleged Frigitemp kickback scheme, according to General Dynamics officials, who also informed the Subcommittee that at this time Veliotis was saying that he had nothing to hide and was prepared to go before the grand jury and testify.[100]

February 1982--General Dynamics officials informed the Subcommittee that Veliotis was saying in February that he was required to be in Greece on matters concerning his recently deceased mother's estate. The GD officials recounted:

> He went to Greece and later reported that he was suffering from inner ear problems and disturbed equilibrium, and could not travel.[101]

February 5, 1982--Assistant U. S. Attorney Denton told Christian Hoffman, an outside counsel for General Dynamics, that Veliotis "was now a potential subject of the grand jury investigation rather than a witness." This information was conveyed to the Subcommittee by General Dynamics officials, who added:

> Denton advised that this change in Veliotis's status had substantial basis in fact. Denton suggested to Hoffman that he examine his client with respect to his sources of income from all over the world.[102]

The Industrial Security Manual (paragraph 6 b.(1)) requires that a defense contractor report to DIS any untoward information it learns about a cleared employee. DIS files reflect no evidence that the specific remarks made by, or the general impression conveyed by, prosecutor Denton were ever reported by General Dynamics officials. The requirement is not that the untoward activity result in an indictment, arrest or conviction--only that it be of a nature that causes concern. Specifically, paragraph 6 b. (1) says:

> Contractors shall submit reports, classified, if appropriate, of any information coming to their attention concerning any of their employees who have been cleared or who are in the process of being cleared for access to classified information, which indicate that such access or determination may not be clearly consistent with the national interest. The subsequent discharge of an individual by the contractor who receives this information does not obviate the requirement to submit this report....[103]

In addition, while there does not appear to be a 6 b.(1)-like requirement calling for the Justice Department to report to DIS potential personnel security problems, the Department must have known what Veliotis's line of work was, the sensitivity of the information to which he had access and the national security implications inherent in the possible conclusion that he had gone bad. The Justice Department particularly, whose jurisdiction includes internal security and domestic counterintelligence, could have alerted DIS to the possibility of Veliotis being a person whose trustworthiness might be in doubt. DIS has not been able to find in its files evidence of any such communication from the Justice Department.

February 20, 1982--In a memorandum on "near term plans" to General Dynamics Chairman David S. Lewis, Veliotis said "personal business affairs which I have been neglecting for a long while" required that he spend a few months in Europe. The press of business--notably Trident and nuclear attack submarine contract negotiations--had prevented him from going abroad earlier and the delay may have been a costly one for him, he said, explaining:

> ...I feel that I can in good conscience take the time off that I need to look after my personal affairs in Europe. I am afraid I may already have waited too long and may have to pay substantial additional taxes that could otherwise have been avoided.

Pointing out that as Executive Vice President for Marine and International Operations he had visited and made improvements in General Dynamics offices in Europe and the Middle East, Veliotis said that in tending to his personal affairs abroad over the next few months he would be available for telephone consultations and expected to "look in on" GD facilities in Egypt, Turkey and Europe. He was, he said, "firmly scheduled" to meet with the President of Greece on March 18 and was prepared to attend "the F-16 ceremony" in Cairo on March 24 if Lewis felt he should. In his absence, Veliotis said, Bill Gorvine, his new deputy, would handle business decisions out of the Quincy office.[104]

February 24, 1982--Veliotis informed the General Dynamics Board of Directors that, effective March 1, 1982, he would be away for "a number of weeks on business."[105]

February 25, 1982--Veliotis attended a meeting of the board in St. Louis.[106]

April 1, 1982--The board met but Veliotis did not attend.[107]

May 1982--Veliotis went to Greece ostensibly to negotiate arms sales for General Dynamics to the Greek Air Force.[108]

May 6, 1982--The board met and reappointed Veliotis as Executive Vice President but he was not present.[109]

February to May 1982--Veliotis spent little time at his offices in Quincy, General Dynamics officials said, adding that on his return on May 6, 1982 Veliotis met with U. S. Attorney's Office representatives in New York and gave them a sample of his writing, had his picture taken, and showed his U. S. passport, preparatory to his appearance before the grand jury. The officials said Veliotis continued to express his willingness to testify.[110]

May 7, 1982--In a telephone conversation, Veliotis told Chairman Lewis that he wanted to take an early retirement. Lewis suggested Veliotis give the matter more thought. Veliotis wrote Lewis a letter of resignation.[111]

May 11, 1982--Veliotis told Lewis on the phone he had not changed his mind about retiring. The letter of resignation had arrived the day before.[112]

May 19, 1982--According to General Dynamics officials, John Gross, attorney for Veliotis, informed company representatives that his client would invoke the Fifth Amendment privilege against self-incrimination if he appeared before the federal grand jury in New York looking into the alleged kickback scheme at Frigitemp.[113]

May 27, 1982--As indicated by a letter to Veliotis from General Dynamics Personnel Relations Vice President Arch H. Rambeau, the company seemed to be treating Veliotis's departure at this time as it might the retirement of any other executive. Rambeau, for example, pointed out to Veliotis that the paperwork was being processed to give him an annuity of about $1500 a month. At his death, his widow Paulette Dupuis would receive about $763 a month. A $1 million Lloyd's of London personal accident policy would be continued at an annual premium of $1200. Another policy, $185,000 in term coverage, would be continued, as would medical protection. A $97,000 check would be mailed to Veliotis as his interest in a "fixed income fund." Veliotis's remaining interest in the fund was about 3900 shares of the company stock, which would also be mailed to him, Rambeau wrote.[114]

June 3, 1982--The General Dynamics Board of Directors accepted Veliotis's resignation as an officer and a director and also accepted his request for early retirement. General Dynamics issued a press release announcing Veliotis's retirement and quoting Chairman David Lewis saying:

> Throughout these years [since 1973] Mr. Veliotis has been a very valued member of the General Dynamics management team. In early 1981, Mr. Veliotis had stated his desire to retire in order to devote substantially full time to the management of his family's business affairs. However, he agreed to stay in his key management position until Electric Boat's commitment to the Navy to deliver the first Trident and six SSN 688-class submarines in 1981 delivery schedules in an outstanding manner. In recent months, he has been concentrating on the company's international activities but he has found that he cannot meet his obligations to his family's business with the heavy travel schedule necessary for the development of General Dynamics's international operations.[115]

General Dynamics's officials would later assert, "The company still had no hard evidence of Veliotis's involvement in kickbacks or commercial bribes" as of this date.[116]

July 30, 1982--F. E. Sussman and Roni Oman, General Dynamics officials, met with Veliotis to discuss his "early retirement benefits," including such issues as savings and stock investment plan distribution, life insurance, medical benefits and options still available to him under the firm's incentive pension plan. It is not apparent from Sussman's memorandum of the meeting as to where it was held.[117]

July 31, 1982--Veliotis signed a security termination statement for the Energy Department, indicating that he had resigned from General Dynamics on the previous June 3 and that his departure had been accompanied by his meeting of all security requirements which departing cleared employees must adhere to.[118] Veliotis signed a similar DOD security termination statement the same day.[119]

September 15, 1982--An Energy Department "file summary sheet" was filled out showing that Veliotis's "Q" access had been terminated on this date. A handwritten notation asserted, "Do not reinstate DOE clearance." It was dated February 15, 1984.[120]

November 1982--According to officials of General Dynamics, at this time the Justice Department gave the firm information alleging that Veliotis had been involved in the reported Frigitemp kickback scheme. General Dynamics officials said their firm began cooperating with the government in further investigations. In a February 18, 1985 letter to the Subcommittee, Robert H. Duesenberg, Vice President and General Counsel at General Dynamics, used the following language to describe how his firm reacted upon learning from prosecutors of Veliotis's alleged participation in the alleged kickback scheme:

> When we were advised by federal attorneys that P. Takis Veliotis was involved in a kickback scheme with one of our suppliers, we took action immediately to cooperate fully with the Justice Department. They were the main investigative agency, but we have cooperated in every way possible with any other federal agency or department in investigations involving this matter.[121]

Summer of 1983--Frigitemp bankruptcy trustee Bernstein filed a civil suit in Delaware, charging that General Dynamics had known of the alleged $2.7 million in kickbacks to Veliotis and Gilliland and that General Dynamics concealed this knowledge to avoid losing its multibillion-dollar Trident submarine contract with the Navy. Bernstein said the "hasty transfer" of the multimillion-dollar subcontract from Frigitemp to IDT, a "totally new, untested corporation," was meant to "perpetuate and conceal the pattern of illegal activities." Bernstein said General Dynamics "had twice promoted" Veliotis while the company knew he was under criminal investigation "in order to insure concealment of the illegal activities."[122]

September 6, 1983--The federal grand jury in New York indicted Veliotis and Gilliland on charges of receiving $2.7 million in kickbacks in connection with the $44 million contract from General Dynamics to Frigitemp. Veliotis was also charged with perjury. The grand jury also indicted Gerald E. Lee and George G. Davis, former officials of Frigitemp. The indictment charged that Davis wired $2.7 million in payoffs for Veliotis and Gilliland to Swiss bank accounts in a scheme that started in 1974. Davis was alleged to have taken another $2 million for himself. The kickbacks also brought contracts to the IDT Corporation, a business set up in 1978 shortly before Frigitemp entered bankruptcy reorganization, the indictment charged. The defendants were also accused of bankruptcy fraud and making false claims with the U. S. Maritime Administration, which subsidized construction of some of the tankers involved. In addition, Veliotis and Gilliland were charged with obstruction of justice because of their testimony in Frigitemp bankruptcy hearings. The indictment said the kickbacks were paid to secure $44 million in subcontracts for insulation work on liquefied natural gas tankers built at General Dynamics's Quincy yard. The four defendants, all charged with a racketeering conspiracy, faced 20-year prison sentences and $25,000 fines. Moreover, if found guilty, they would be required to relinquish any interest in Frigitemp, General Dynamics, IDT or a series of fictitious businesses created in the Cayman Islands to aid the alleged kickback scheme. William M. Tendy, Chief Assistant U. S. Attorney in the Southern District of New York, said that General Dynamics had assisted the government in its inquiry leading to the indictments.[123]

September 14, 1983--According to General Dynamics officials, they filed the first of three law suits against Veliotis aimed at attaching his holdings in the U. S. and Canada. The other two suits were filed on October 25, 1983 and November 14, 1983.[124]

November 16, 1983--George Veliotis, the brother of P. T. Veliotis, committed suicide, one day after he had received a subpoena to give a deposition in a General Dynamics civil suit, General Dynamics officials said. Also on this day, GD officials said, Takis Veliotis filed a $142 million damage suit against General Dynamics. The firm's officials said Veliotis dropped the suit on January 24, 1985.[125]

January 1984--Gerald E. Lee, former Frigitemp chairman, pleaded guilty to conspiracy charges in the kickback case stemming from the Southern District of New York grand jury inquiry. George G. Davis, the second Frigitemp executive indicted, denied the charges at his arraignment. Gilliland was reportedly in jail in England awaiting extradition. Veliotis reportedly was living in comfort in Athens and there was little likelihood of his extradition.[126]

January 1984--Veliotis, a fugitive, reportedly had offered the government a deal whereby he would provide information about General Dynamics's alleged use of fraudulent claims to reap hundreds of millions of dollars from the Navy in submarine construction cost overruns. In return, Veliotis reportedly wanted immunity from prosecution regarding his own conduct while a General Dynamics official. Veliotis was said to have declared that GD officials deliberately underbid the contract they won from the Navy in 1971 to build the SSN 688 submarines. Veliotis reportedly said that the settlement through which the Navy agreed to the firm's claims was based on fraudulent data.[127]

February 20, 1984--Newsweek recounted rumors that Veliotis threatened to provide the Soviet Union with secret information about the U. S. submarine fleet. The rumors were not corroborated. Newsweek reported:

> More alarming are the rumors that Veliotis threatened to provide the Soviet Union with some of the most sensitive secrets of the U. S. submarine fleet. Besides supervising the construction of the SSN 688 and the Trident submarines, he had clearance to receive top secret information. Sources close to the fugitive deny that he has ever made any such threat, but Newsweek has learned that both General Dynamics and the Navy have investigated whether Veliotis ever obtained information about submarine nuclear systems or the "acoustics" that permit them to run silently to evade Soviet hunters. There is no direct evidence he did, but intelligence agents are watching him closely. Says a senior Navy official, "we can't rule out the possibility that he may still have agents in the construction process and that he may have stolen some documents."[128]

February 26, 1985--A Department of Energy official was interviewed by Subcommittee Assistant Counsel John Sopko and Investigator Leonard Willis on the subject of Veliotis's having been granted a "Q" access authorization in 1977. The official acknowledged eight failures in the Veliotis matter, including 1) a failure by Energy to find out more about Veliotis's unreported trip to Russia in 1973; 2) a failure by Energy to reconcile the conflict in dates between Veliotis's 1953 emigration to Canada and the 1954 conviction for money order fraud in Greece; 3) a failure by Energy to find out more about the 1954 conviction to determine if it was or was not sufficiently serious to justify denial of the "Q" request; 4) a failure by Energy to demand that no adjudicative action be taken on Veliotis until it was established that the person convicted in Piraeus in 1954 was or was not the same person who emigrated to Canada in 1953; 5) a failure by Energy, as well as DOD, adjudicators to insist upon more direct evidence of the facts and place of Veliotis's birth; 6) a failure by Energy adjudicators to require confirmation of Veliotis's assertions about his formal education in Greece; 7) a failure by Energy adjudicators to require a personal interview of Veliotis to confront him with the inconsistent information in his past; and 8) a failure by Energy to adhere to the special investigative-adjudicative requirements for aliens applying for "Q" access authorization as spelled out in detail in AEC Appendix 2301. The official added that the FBI report that noted the June 7, 1954 conviction of Veliotis in Piraeus contained contradictory information because it also referred to Veliotis's claim that he emigrated to Canada in 1953. The senior Energy Department official was asked about Veliotis's frequent assertion in government personnel security forms in which he said he graduated with a "B.A." degree from St. Paul's College in Piraeus in 1942, which would mean he got his degree at the age of 16. The official said the FBI report indicated that an effort was made to verify Veliotis's attendance at and graduation from St. Paul's College but that the school had been damaged during World War II, destroying pertinent records. A similar excuse was given in 1973 when DIS tried but failed to verify Veliotis's reported graduation from Athens University. Another confidential source, who has read the FBI files, said the Bureau reported to Energy that Veliotis had enrolled in the Greek naval academy but had not earned a degree there. The senior Energy Department official also refuted a statement made by Admiral Rickover in the August 2, 1977 letter to Energy Department security chief Harvey Lyon. Admiral Rickover wrote that in processing Veliotis's "Q" access authorization "the requirements of Appendix 2301 appear to be satisfied." The Energy official disputed that, saying Appendix 2301 requirements were not met.[129]

February 26, 1985--The *St. Louis Post-Dispatch* reported that Veliotis had disclosed to Justice Department officials in Athens that F. G. Tovar, who had succeeded him as General Manager at Groton, had given classified information about the Trident submarine to persons who had no security clearances in late 1982 and early 1983. The *Post-Dispatch* article said the Justice Department was investigating whether or not Tovar or General Dynamics violated DOD regulations governing the protection of classified information.

Neither Veliotis nor sources familiar with the investigation would say precisely what Trident information was disclosed or give further details, the paper reported.[130]

February 27, 1985--CBS television news reported that the Justice Department was investigating reports that sensitive information about Trident submarine technology had been diverted from the General Dynamics Electric Boat Division. No other information was provided by the news organization. Dan Rather reported:

> New allegations tonight about the nation's largest defense contractor, General Dynamics, whether that company has a security breach problem with one of this nation's top of the line front-line weapons, the Trident submarine. CBS News reporter Rita Braver, in Washington, has learned that a company document containing classified Trident information has gotten outside the company, documents that some say could give anyone who got hold of them a good idea of the Trident's maximum speed and other specifications....[131]

March 1, 1985--Robert H. Duesenberg, Vice President and General Counsel for General Dynamics, acknowledged to Subcommittee Investigators Glenn Fry and Fred Asselin that Veliotis's employment form--the basic job application each employee must submit before being hired--is inexplicably missing from GD files. Duesenberg said he had no idea of how the document could have disappeared or when the loss occurred. Unless the form is found, we will not be able to evaluate the information Veliotis provided about himself to General Dynamics.[132]

March 11, 1985--Veliotis was reported to have given Justice Department officials a copy of a General Dynamics internal financial report that contained 19 highly sensitive pictures of a Trident submarine. When the chief of Navy shipbuilding saw the pictures, he accused General Dynamics of losing control of information "damaging to the national security," according to the Washington Post, which went on to say that Vice Admiral Earl B. Fowler had been shown the pictures as part of a damage assessment to determine how much the Trident's secrets might have been compromised. The Post reported that the CIA had also assessed the extent of the possible Trident information compromise and was similarly troubled by the publication of the photographs. One analyst was quoted as having said, "Oh, my God, we would love to have those kind of photographs of their [Soviets'] submarines."[133]

March 22, 1985--The possibility that Veliotis might be a spy as well as a kickback artist, raised by Newsweek in 1984, surfaced again in a New York Times article of this date which reported that CIA officials were concerned about the broad knowledge Veliotis possessed about American submarines. Veliotis, expressing strong pro-American and anti-Soviet views, reportedly dismissed as groundless anyone's fears that he might have sold secrets to the Soviets. Here was how the Times reported this issue:

A man with rigidly anti-Soviet politics and an acknowledged affection for the American way of life, Mr. Veliotis tolerated no suggestion that he might be perceived in the United States as a security risk. His broad technical knowledge of Navy submarines is known to be of concern to the Central Intelligence Agency. But though he discussed ways in which he believes Soviet submarine technology may be ahead of American designs--mostly due, he charged, to Navy reluctance to try new techniques--he dismissed the CIA's fears.[134]

FOOTNOTES

1. Form G-325A, Biographic Information, Immigration and Naturalization Service, on Panagiotis Takis Veliotis, May 9, 1973; Form AEC-1, Personnel Security Questionnaire, Atomic Energy Commission, June 28, 1977; and DD Form 49, Personnel Security Questionnaire (Industrial), Defense Department, December 27, 1972. (DOE, DOD) (Parenthetical acronyms reflect source of documents.)

2. June 28, 1977 AEC Form.

3. Ibid.

4. In August of 1981, Dome Petroleum, Ltd., Calgary, Canada, acquired Davie Shipbuilding, according to Moody's International Manual, 1984 Vol. 1, p. 791.

5. Who's Who in America, 42nd edition, 1982-1983, Vol. 2, p. 3420.

6. David S. Lewis, Chairman and Chief Executive Officer, General Dynamics Corporation, letter to Harvey E. Lyon, Director, Division of Safeguards and Security, Energy Research and Development Administration, July 26, 1977; Lewis letter to Admiral C. R. Bryan, Commander, Naval Sea Systems Command, July 25, 1977. (GD, DOE)

7. Energy Department summary statement, apparently used by the Department in adjudicating Veliotis's 1977 application for a "Q" access authorization, wherein it was noted that, according to an FBI memorandum of August 26, 1977, Veliotis "rec'd 45 days imprisonment in accordance with Decision #10 of June 7, 1954 in Piraeus Court of Misdemeanor for issuance of 'uncovered money orders.'--not listed." (DOE)

8. December 27, 1972 DOD form.

9. "Resume of Panagiotis Takis Veliotis." (GD)

10. Quoted in Allan Dodds Frank, "The One That Got Away," Forbes, January 16, 1984, pp. 31-33.

11. E. S. Perkin, Director of Industrial Security, Department of Defence Production, Canadian Government, letter to G. L. C. Bates, Chief Security Officer, Davie Shipbuilding, Ltd., Lauzon, Levis, Province of Quebec. (GD)

12. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Second Report, Vol. 2, August 1981, pp. 797, 798.

13. L. Z. Robitaille, Naval Ship Systems Command, memorandum to Naval Material Command, November 21, 1967; and S. K. Mansfield, Naval Material Command, memorandum to Defense Contract Administration Services Region, Boston, November 27, 1967. (GD)

14. Harry Anderson, "Beware of Greeks Bearing Secrets," Newsweek, February 20, 1984, pp. 58, 59, 61; and information provided Subcommittee by General Dynamics, February 6, 1985.

15. Jane's Fighting Ships 1983-84, pp. 633, 634, 636.

16. Form ERDA-354, Data Report on Spouse, filed by Veliotis, June 28, 1977. (DOE)

17. "General Dynamics Taps Veliotis As Manager Of Quincy, Mass. Unit," unsigned Wall Street Journal article, December 22, 1972.

18. Paul R. Ray letter to Algie A. Hendrix, Vice President for Industrial Relations, General Dynamics, October 31, 1972, with attachments. (GD)

19. Hilliard W. Paige, President, General Dynamics Corporation, notarized letter to Veliotis, November 7, 1972. (GD)

20. Wall Street Journal article, December 22, 1972.

21. December 27, 1972 DOD form.

22. Information provided Subcommittee by General Dynamics, December of 1984.

23. General Dynamics press release, January 1973. (GD)

24. Memorandum prepared at Subcommittee's request by Holly Kenworthy, Foreign Affairs Analyst, Central Research Section, Foreign Affairs and National Defense Division, Congressional Research Service, Library of Congress, March 21, 1985. This memorandum may also shed light on questions about Veliotis's assertion in government documents that he earned a "B.A." degree from St. Paul's College in Piraeus. According to Kenworthy, Piraeus reportedly had a "Greek-French School of St. Paul" and an "Ecole St. Paul," the latter being near Afentouli Street where Veliotis said his father's business was located. Kenworthy said it is possible that when he wrote "B.A." under the question of degrees earned, he meant to signify "baccalaureate," the degree which is earned in many Greek high schools where studies go on for six years as opposed to the four-year curriculum in the U.S. Kenworthy said, "A French expert asserts that the abbreviation for baccalaureate is 'bac,' but also claims that many Europeans consider the 'bac' to be a bachelor's degree and therefore write B.A."

25. Fred Asselin, Investigator, Senate Permanent Subcommittee on Investigations, letter to Mark Lowenthal, Foreign Affairs and National Defense Division, CRS.

26. "Across Canada," unsigned article in *Toronto Globe and Mail*, March 2, 1983, p. 9.

27. F. R. Ryan, Manager, Plant Protection, Quincy Shipbuilding Division, memorandum to R. M. Smith, et al., January 4, 1973. (GD)

28. Bernard J. Finn memorandum, January 10, 1973. (GD)

29. Information provided by General Dynamics.

30. Bryan memorandum to Supervisor of Shipbuilding, Conversion and Repair at Electric Boat, January 16, 1973. (GD)

31. J. R. Burns, Director of Nuclear Engineering, Electric Boat, letter to Bryan, February 13, 1973. (GD)

32. Colonel David T. Clark, USA, Chief, Office of Industrial Security, Contract Administrative Services, Defense Supply Agency, memorandum to Defense Logistics Agency, Boston office, February 16, 1973. (GD)

33. P. G. O'Keefe, Supervisor of Shipbuilding, Conversion and Repair, USN, Groton, memorandum to Naval Ship Systems Command, February 21, 1973. (GD)

34. D. G. Gigizas, Mayor of Kranidion, Greece, statement concerning year and place of Veliotis's birth, dated February 26, 1973; Berlitz translation, dated March 13, 1973. (GD, DOE)

35. Gorden E. MacDonald memorandum to Lewis, March 28, 1973. (GD)

36. Department of Defense National Agency Check Request on Veliotis, May 18, 1973. (DOD)

37. DIS Special Agent R. W. Magill, Report of Investigation regarding Veliotis, June 7, 1973. (DOD)

38. DOD National Agency Check, in Veliotis inquiry, May 18, 1973. (DOD)

39. Patrick Toomey, District Director, INS, Boston office, letter to Veliotis, June 13, 1973. (DOE)

40. Paul Moses, Associated Press, "Two Ex-General Dynamics Execs Indicted," as article appeared in *Schenectady Gazette*, September 7, 1983.

41. DIS S/A L. D. Gianascol, Report of Investigation regarding Veliotis, July 12, 1973. (DOD)

42. DIS S/A B. J. Haupt, ROI regarding Veliotis, with sworn statement, July 16, 1973. (DOD)

43. DIS S/A A. J. Pfeiffer, ROI regarding Veliotis, July 27, 1973. (DOD)

44. Jonathan D. Makris, Special Agent in U. S. Air Force Office of Special Investigations serving in Europe, ROI regarding Veliotis, August 9, 1973. (DOD)

45. DIS S/A F. P. Boyda, ROI regarding Veliotis, August 31, 1973. (DOD)

46. Magill, ROI regarding Veliotis, August 31, 1973. (DOD)

47. DIS S/A K. R. Doktor, ROI regarding Veliotis, September 7, 1973. (DOD)

48. AEC Personnel Security Questionnaire, filed by Veliotis, June 28, 1977, supplemental to question No. 13 on foreign travel. (DOE)

49. DOD, *Industrial Security Manual For Safeguarding Classified Information*, 6-b (9), pp. 35, 36, March 1984.

50. DIS S/A P. C. Miller, ROI regarding Veliotis, September 17, 1973. (DOD)

51. Defense Industrial Security Office, letter of consent to Security Officer of Quincy Division on Veliotis's secret clearance, January 23, 1974. (GD, DOE)

52. J. L. Budros, Corporate Director of Security, General Dynamics, memorandum to Hendrix, January 24, 1974. (GD, DOE)

53. Warren G. Sullivan, Vice President for Industrial Relations, General Dynamics, letter to Vice Admiral Robert C. Gooding, Commander, Naval Sea Systems Command, October 22, 1975. (GD, DOE)

54. Gooding letter to Sullivan, November 14, 1975. (GD, DOE)

55. Sullivan letter to Gooding, December 3, 1975, with Veliotis affidavit. (GD, DOE)

56. General Dynamics press release, Veliotis biographical sketch, December 1975. (GD)

57. Alfred E. Dupell, Director, Security Division, Naval Sea Systems Command, letter to Ryan, February 3, 1976. (GD)

58. General Dynamics information February 6, 1985.

59. AEC Veliotis form June 28, 1977.

60. Charles Middleton, General Dynamics Corporation official, memorandum to Edward E. Lynn, GD General Counsel, July 19, 1977. (GD)

61. Lewis letter to Bryan, July 22, 1977. (GD, DOE; copy provided by Energy Department is dated July 25, 1977.)

62. Arch H. Rambeau, Director of Personnel and Management Relations for General Dynamics, memorandum, July 25, 1977. (GD, DOE; General Dynamics copy dated July 22, 1977.)

63. Lewis letter to Bryan, July 25, 1977.

64. AEC Veliotis form June 28, 1977.

65. Admiral Hyman G. Rickover, Director, Division of Naval Reactors, ERDA, letter to Lyon, August 2, 1977. (DOE)

66. William H. Walsh, Director, Safeguards and Security, Schenectady Naval Reactors Office, request for investigation on Veliotis, sent to FBI's Employees Security and Special Inquiry Section, August 5, 1977. (DOE)

67. Lyon letter to Rickover, October 13, 1977. (GD, DOE)

68. B. M. Erickson, Manager of Naval Reactor Office in Schenectady, letter to Electric Boat, October 19, 1977. (DOE)

69. DOE summary for "Q" on Veliotis.

70. Energy Department file summary sheet, apparently used by Department in adjudicating Veliotis's application for "Q" access, wherein it was noted that "arrest 25 years ago not listed," September 29, 1977. (DOE)

71. Lewis memorandum to "Division Managers, Subsidiary Presidents and Corporate Officers," October 21, 1977. (GD)

72. Quoted in Frank, January 16, 1984.

73. R. E. Nehls, Director of Industrial Security, Defense Logistics Agency, Boston, letter to Veliotis, October 28, 1977. (GD)

74. Vincent M. Pusateri, Chief, Personnel Security Branch, Security and Safeguards, Energy Department, memorandum to M. J. Dowd, Chief, Internal Security Branch, December 5, 1977. (DOE)

75. General Dynamics information, February 6, 1985.

76. Jeff Gerth, "General Dynamics' Eligibility On Contracts Studied By Navy," New York Times, December 21, 1983, p. D4.

77. Ibid.; and Allan Dodds Frank, "Sherlock Bernstein," Forbes, January 30, 1984, pp. 35, 36.

78. Anderson, February 20, 1984.

79. Ibid.

80. Ryan letter to Energy Department, May 8, 1979. (DOE)

81. J. W. Rannenberg, Director of Contracts, Electric Boat, letter to Supervisor of Shipbuilding, Conversion and Repair, USN, January 1980; with December 5, 1979 conference report by Groton Manager of Industrial Security. (GD)

82. General Dynamics press release, February 8, 1980. (GD)

83. C. R. Roberts, office of the Supervisor of Shipbuilding, Conversion and Repair, USN, memorandum to Defense Logistics Agency, February 14, 1980. (GD)

84. Anderson, February 20, 1984.

85. Patricia A. Hill, Contracting Officer for Security Matters, Naval Sea Systems Command, memorandum to Defense Logistics Agency, March 4, 1980. (GD)

86. Wesley W. Parks, Acting Chief, Technical Support Division, Directorate of Industrial Security, Defense Logistics Agency, letter to F. R. Ryan, March 12, 1980. (GD)

87. DISCO letter of consent to Electric Boat on Veliotis's top secret clearance, March 12, 1980. (GD)

88. Dale L. Hartig, Chief, Office of Information and Public Affairs, DIS, letter to Fred Asselin, with attachment, March 21, 1985.

89. General Dynamics information, February 6, 1985.

90. Ryan letter to Defense Logistics Agency, September 15, 1980. (GD)

91. Parks letter to Ryan, September 29, 1980. (GD)

92. Anderson, February 20, 1984.

93. General Dynamics press release, October 5, 1981. (GD)

94. General Dynamics information, February 6, 1985.

95. Patrick E. Tyler, "General Dynamics Inquiry Reported," Washington Post, January 17, 1984, p. 1.

96. General Dynamics Incentive Compensation Review on Veliotis. (GD)

97. Frank, January 16, 1984.

98. Confidential information.

99. General Dynamics information, February 6, 1985.

100. Ibid.

101. Ibid.

102. Ibid.

103. Industrial Security Manual, March 1984, p. 33.

104. Veliotis memorandum to Lewis, February 20, 1982. (GD)

105. General Dynamics information provided the Subcommittee, June 7, 1984.

106. Ibid.

107. Ibid.

108. Anderson, February 20, 1984.

109. General Dynamics information, June 7, 1984.

110. General Dynamics information, February 6, 1985.

111. General Dynamics information, June 7, 1984.

112. Ibid.

113. General Dynamics information, February 6, 1985.

114. Rambeau letter to Veliotis, May 27, 1982. (GD)

115. General Dynamics press release, June 3, 1982. (GD)

116. General Dynamics information, February 6, 1985.

117. F. E. Sussman, Quincy yard official, memorandum to Roger Groh, July 30, 1982. (DOE)

118. Security Termination Statement, Energy Department, Veliotis, signed July 31, 1982. (DOE)

119. Security Termination Statement, DOD, Veliotis, signed July 31, 1982. (GD)

120. Energy Department file summary sheet on Veliotis, September 15, 1982, with February 15, 1984 notation. (DOE)

121. Robert H. Duesenberg, Vice President and General Counsel, General Dynamics, letter to Asselin, February 18, 1985.

122. Gerth, December 21, 1983.

123. Moses, September 7, 1982.

124. General Dynamics information, February 6, 1985.

125. Ibid.

126. Anderson, February 20, 1984.

127. Ibid.

128. Ibid.

129. Subcommittee staff memoranda (sealed).

130. Jon Sawyer and William Freivogel, "Pattern of Fraud By Firm Alleged," St. Louis Post-Dispatch, February 26, 1985, p. 1.

131. Dan Rather, CBS Evening News, as quoted in Radio-TV Defense Dialog, Radio TV Reports, Inc., Washington, D. C., February 28, 1985.

132. Staff memorandua (sealed).

133. Tyler, "Navy Accuses Sub Builder Of Security Breach," Washington Post, March 11, 1985, p. 1.

134. Wayne Biddle, "General Dynamics' Accuser," New York Times, March 22, 1985, p. D1.

Exhibit No. 13

SUMMARY STATEMENT

NMC

Panagiotis T. Veliotis	Ac 59111	QF
Name	AEC#	Type of Clearance

Pres & Gen Mgr - General Dynamics

DEROGATORY	MITIGATING
FBI 9/13/77 Alexandria, Va	
	CIA - no identifiable info concerning subject or his immediate family.
SI 9/12/77 Boston, Mass.	
	Employed Gen Dyn - Quincy 1/73 - favorable
	Reference Hanson A Reynolds attorney for subj is handling his INS papers. Recommends on his limited contact.
	Reference Louis H Weinstein has known subj since 1973. Outstanding man who values principles of American democracy. Recom
	Three neighbors with limited contact - recommend.
9/7/77 Cincinnati	DISCO issued Secret clearance 1/23/74 based on BI by DIS dtd 11/1/73.
9/6/77 Milwaukee	C. Lee Spear, references, has known subj 20 yrs. Based on his business association he recommends. Considers subj loyal to U S in all matters

Ac 59111

Panayotis P. Velotis
FBI Memo dtd 8/26/77
Subj rec'd 45 days imprisonment in accordance with Decision #10 of June 7, 1954, in Piraeus Court of Misdemeanors for issuance of "uncovered money orders." – not listed

PSQ dtd 6/28/77
Born Citizen of Greece
Present citizenship: Canadian
Date of Entry 6/11/73
Port of Entry Boston
Alien Reg # A 19-350-869

— —

Lyons's Ltr dtd 8/2/77 from Rickover
Permanent immigrant alien 6/73
Filed Declaration of Intent to become Citizen per 7/28/77
Eligible to become citizen of US 6/78. —

HHc c̄ There is no reports in FF to substantiate – Dec. of Intent sent to INS

Senator NUNN. Our next witness is Mr. Phillip Parker who is Deputy Assistant Director, Intelligence Division, Federal Bureau of Investigation.

You have some associates with you. If you are going to testify and be available for questions, would you hold up your right hands and take the oath as all our witnesses do?

Do each of you swear the testimony you will give before the subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. PARKER. I do.

Mr. PORTER. I do.

Mr. DOMZALSKI. I do.

Senator NUNN. We appreciate you being here today. We have questions for you. You have an opening statement. To the extent you can summarize, it would be appreciated. You might want to introduce your colleagues with you.

TESTIMONY OF PHILLIP A. PARKER, DEPUTY ASSISTANT DIRECTOR, INTELLIGENCE DIVISION, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY JOSEPH D. DOMZALSKI, ASSISTANT SECTION CHIEF, CIVIL RIGHTS AND SPECIAL INQUIRY SECTION, AND HARRY W. PORTER III, UNIT CHIEF, INTELLIGENCE DIVISION, NON-SOVIET RESEARCH AND ANALYSIS

Mr. PARKER. On my left is Special Agent Harry Porter with our Intelligence Division. On my right is Special Agent Joe Domzalski with background in the special inquiry section.

I am very happy to be here today. We welcome the opportunity to speak with you about our Government and contract employees with access to classified or other sensitive data who may commit espionage.

There are approximately 2,600 Communist country officials assigned to the Soviet bloc, Cuban, diplomatic and commercial facilities in the United States. We consider about 30 percent of these individuals to be connected with the intelligence services of those countries.

One of the greatest achievements any intelligence service can have is the recruitment of an agent in a national-defense related facility or the penetration, recruitment of an agent in a private institution where national-defense related research and development work is performed.

Recruited agents who don't have the access can also be used to spot those people who do have the access to the classified material. Safeguarding classified material is a very difficult job. There is no question about it. We have to consider the areas in which research and development generate sensitive information.

The collection mission of the intelligence service centers on the assessment and development of employees of the defense-related industry.

I think Sergeant Smith very eloquently put forth the effort that they place in developing the agents. The method that he presented, that of a hostile intelligence service officer meeting, getting to know and eventually recruiting an American or an individual who has access to our defense-related information from disgruntled or perhaps mentally disturbed individuals who are already employed in sensitive areas. They take advantage of the emigre population in the United States. Special establishments in the United States run by the various Soviet and Soviet bloc nations serve as excellent cover organizations in their collection effort.

Money and revenge seem to be the two basic motivators of those who are ready to commit espionage. Others may be drawn into espionage believing that they are serving a cause other than the actual cause that is being presented; a false-flag type approach.

There are variations of how they go about it. We find espionage springing from financial difficulties, greed, professional or personal problems. In varying degrees, many of these problems may be detected and resolved before a person commits himself or herself to espionage.

We have discussed with your staff a number of cases where classified information was obtained by hostile services. I have with me today for the record summaries of these cases and others that I believe will illustrate clearly the methods used by those services. There are many reasons why a person chooses to commit espionage, and I think these summaries show the basic motivation. Some of these cases are William Holden Bell; James Harper; William Peter Kampiles; Edwin Moore; Andrew Lee and Christopher Boyce; Ronald Humphrey and Thomas Patrick Cavanagh, and there are numerous others.

One of the things that we must insist on is that each Government agency or contractor have a specific official responsible for security matters. This individual must be recognized as an ally and not an adversary of the employees. He must have training and the time to perform his duties.

In those cases where an intelligence officer has developed a social relationship with an individual, the security officer's job is to minimize the damage, protect the employee and extricate him, if possible, without further loss. We would hope at the time the security officer has learned that one of the employees is in contact with a hostile service officer, he come to the FBI and provide us with that information. We do carry out a program we call DECA, Development of Counter-Intelligence Awareness, in which we go to the various contractors, defense-related contractors and point out to their security officers and other officials within the company the threat that does exist from all of the hostile services located in the United States and how best to prevent the loss of classified information through a human recruitment.

If I might add, we—the FBI—are not counter-measure specialists. We are not ready to go to a factory and tell you how many safes you need; how high your fence should be; or how thick the doors should be. That is not our business. We're here to counteract, to prevent the hostile intelligence service officer from doing his job. He does his job by recruiting agents to work for him. Once the agent is recruited, and he is able to have access to the information within a particular facility, the security precautions that are followed by the company and enforced by the security officer should be sufficient to prevent that individual from walking out with classified information.

One of the most important steps that the facility can have is a requirement that all employees who have dealings with foreign country representatives report those contacts to the security officer. I'm not saying hostile foreign services; I'm saying foreign services because, again, the false-flag approach is certainly something the Soviets and Soviet-bloc services have used. It is very difficult for an individual to determine the difference between an East German and a West German. For that matter, from a Soviet intelligence officer who is fluent in many languages from a French businessman.

We also strongly endorse a system that improves the physical security of facilities. We must have control of access areas, document accountability procedures and after-hours access approvals so that some one who wishes to go in on a Saturday or evening must have the approval of the appropriate security official before they can get in.

The security officer's role must be stressed. He and his staff face the broad threat from intelligence officers and their agents residing in the United States visiting commercial, scientific, technical delegations; the emigre population that is rapidly approaching the time that they will be eligible for citizenship and the disgruntled, unhappy employee or perhaps one who has mental problems should be and must be recognized by the security officer.

Other steps can be taken. I am referring to the pre-employment background investigation; update of agency checks and strong facility security programs and, most of all, a continuing awareness briefing of all employees by the security officer.

Our Administrative Services Division is responsible for hiring all FBI personnel. Because of the large number of applicants versus the limited number of vacancies, this is carried out on a very limited basis. The application process for each applicant appointed is lengthy, detailed and enters around testing, personal interviews and exhaustive background investigation that must meet requirements to grant security clearance up to and including top secret. Results of these items are scrutinized by case analysts and two to three levels of special agent supervisory personnel.

In situations of admitted or developed contacts or relations with individuals in foreign countries, we check CIA's files and, if necessary, we go to the local service overseas. If necessary, we do ask that the applicant be polygraphed. The polygraph may also be required in other types of situations in order to resolve questionable items discovered in the background investigation.

Our application form is very detailed, and the applicant must complete it fully. We check our own records; check all local police, school—any records that are available to us on our applicant. We try to get as much information which will give us a reading on his character, his associates, his reputation, loyalty, skills and any other factor that may have some bearing on the job that he is applying for. Any new or questionable information developed is fully explored and resolved.

We do background investigations for other agencies. Executive Order 10450 is the basis for these investigations. The names of the potential Government employees are searched through records at FBI Headquarters, including fingerprint files.

In addition, background investigations are conducted for a limited number of agencies when requested in writing. Those presently served by the FBI are the White House, including National Security Council; the Department of Justice; the Department of Energy; the Administrative Office of the U.S. Courts and certain congressional committees.

The investigation and file reviews are designed which will develop any information which would reflect on one's suitability for Government employment or for security clearance purposes. The FBI provides the fully developed facts, particularly in regard to unfavorable information or other areas of concern, to the client agencies who have responsibility for making employment or access determination.

The FBI does not make the recommendations to those agencies for or against employment or clearance. Also, many agencies provide the periodic update which affords an opportunity for re-examination of a person's background and for the development of any information which could have an adverse impact on continued employment with the Government.

The investigation encompasses an individual's adult life from age 18 and includes inquiries concerning residences, education, employments, military service, credit and arrest records. We interview coworkers, former neighbors, neighbors, supervisors, professors, roommates, references and associates in an effort to develop comments concerning his suitability for Federal employment.

Although the same general scope is applied to each investigation, the background of an applicant is carefully analyzed in an effort to identify areas where particular emphasis, based on that person's unique history, should be placed.

Senator NUNN. Could I ask a question here? We heard testimony about the Office of Personnel Management doing investigative reports. We heard testimony about DIS, Defense Investigative Service, and we have heard reports about State Department having their own investigation and the FBI, of course, has background investigative responsibilities in certain areas. How do you and the FBI decide whether you are going to honor a request for an investigation from another agency? What are your rules? When does the FBI have jurisdiction over these as opposed to all these other agencies? Give us an idea, and maybe you can furnish for the record whatever rules and regulations you have.

Mr. DOMZALSKI. Essentially, Senator, we have no specific authority to do the investigations for other agencies. They are being done at the request of those agencies, and we have honored those requests. For the Department of Justice——

Senator NUNN [interposing]. In other words, when they get to deciding they want you to do one, they get you to do one; if they want DIS to do one——

Mr. DOMZALSKI [interposing]. Again, certain agencies have arranged for us to do the investigations. The Department of Justice, the Attorney General has specified positions in the Department of Justice which require an FBI background investigation.

Starting around President Eisenhower's time, we've conducted investigations for Presidential appointments and members of the White House Staff at the request of the President. Certain congressional committees have arranged through the Attorney General for the FBI to do background investigations on staff members when they require access to classified information.

So there is no requirement that it be the FBI to do these investigations. However, determinations have been made by the Attorney General and the President that they want the FBI to do them.

Senator NUNN. What about the Department of Energy? You have a relationship with them, don't you?

Mr. DOMZALSKI. Yes, we do. Under the Atomic Energy Act of 1954, there is provision in there for positions which the commissioners at that time determined to be important and sensitive to be investigated by the FBI. That is one area where there is a specific statutory requirement that an FBI investigation be conducted.

Senator NUNN. Do you have any coordination with any of the other investigative agencies in the sense you decide when it is appropriate for you to undertake one or when it is appropriate that they take one? Is there any kind of liaison between you and DIS and the Office of Personnel Management, get common techniques, common approaches, anything like that going on?

Mr. DOMZALSKI. We have been associated with all of the investigative services and have discussed what is necessary in terms of background investigations. We served on joint committees with them which have examined the personnel security systems and the requirements of background investigations in the past and exchanged views as to what one agency does as opposed to what another agency is doing. So there is cooperation that goes on.

Senator NUNN. Do you have difficulty—other agencies have complained about the lack of access to State and local criminal records. Of course, you coordinate more extensively than other agencies in other endeavors. Do you have any difficulty getting State 5and local support in your background investigations?

Mr. DOMZALSKI. I think we have had less difficulty than the other agencies because overall, we are a criminal justice agency and have daily contact with these agencies. There have been some cases where we have had to go out and sit down and work out arrangements with them to have access regarding applicant investigations.

Senator NUNN. But when you do that, you are doing it only for the FBI; you are not doing it on behalf of——

Mr. DOMZALSKI [interposing]. On behalf of the other services? No.

Senator NUNN. Excuse me, Mr. Parker. Go ahead.

Mr. PARKER. Thank you, Senator. To mention briefly, background investigations abroad, we have no authority to conduct background investigations overseas. Where such investigations require checking foreign police, domestic security or intelligence organization records our legal attachés through established channels request that information, we must rely on whatever information is provided. We are not in the position to verify or otherwise confirm information provided by the host country.

Senator NUNN. So basically you just have to accept whatever you get from that country without really questioning them?

Mr. PARKER. We can, if there is something that we see in the information that we receive that could perhaps be amplified upon, we would go back to that organization, but still we are completely limited to how much information they are willing to give us.

Senator NUNN. Is that a fatal flaw in the whole investigative capability when foreign nationals are applying for security clearance here, people who have recently been made American citizens, is this a fatal flaw or would you describe it as a serious problem, or would you just say it is a problem? How would you describe it?

Mr. PARKER. In the first place, with the European NATO countries, we have no reason to doubt the information that they give us. We have excellent relationships with those countries and with their organizations.

Senator NUNN. How about Greece?

Mr. PARKER. I have no reason to doubt, to question information that they would give us.

Senator NUNN. How about the Veliotis case?

Mr. PARKER. I cannot comment on that one, Senator, on that particular case. I will say that any foreign country is going to be somewhat circumspect in providing information to another country depending upon the use that is going to be put to that information. If it is of a sensitive nature, I think you will realize that country has a right to be somewhat hesitant about providing information that may deal with sources or methods of particular intelligence organizations.

Senator NUNN. So are you saying this is not a big problem, just as long as it applies to NATO countries?

Mr. PARKER. I think we have very good relationships with them and within the limitations of any dissemination of information, it doesn't seem to be a great problem to me.

Senator NUNN. How about Eastern bloc countries?

Mr. PARKER. Well, I would certainly not go to an Eastern bloc country and ask them for a background check.

Senator NUNN. How do you handle that?

Mr. PARKER. I'm not at liberty to discuss that here, Senator, but I would be happy to provide you with an answer to that. I think we have procedures, while certainly not foolproof, to give us an ability to conduct somewhat of a background investigation in those areas.

Senator NUNN. Is it less than satisfactory?

Mr. PARKER. Much less than satisfactory.

Senator NUNN. We will get into the techniques in a closed session or in private, but you are saying that is a real problem?

Mr. PARKER. Absolutely.

Senator NUNN. And that is much more of a problem than NATO countries——

Mr. PARKER [interposing]. Yes, sir. Any emigre or any investigation of an emigre from an Eastern bloc, Soviet bloc country raises problems that are almost insurmountable.

Senator NUNN. Almost insurmountable?

Mr. PARKER. Yes, sir.

Senator NUNN. I have a list here of those either cleared from these countries or in process of being cleared. That is just for the information of those interested.

Albania, 17; Bulgaria, 55; Cambodia, 24; People's Republic of China, 3,291; Cuba, 1,056; Czechoslovakia, 574; North Korea, 51; East Germany, 257; Hungary, 947; Laos, 14; Poland, 1,225; Romania, 354; U.S.S.R., 1,555; Vietnam, 670; Yugoslavia, 585, giving a total of 10,675 from basically behind the Iron Curtain.

Mr. **Parker**. Yes, sir.

Senator **Nunn**. And you are saying we have no real good way of checking on the background?

Mr. **Parker**. On a background investigation; that's correct, Senator. If I might say, these people, though, are extremely bright and can contribute very much to the United States.

Senator **Nunn**. I understand that. It's a dilemma.

Mr. **Parker**. The problem is in conducting the background investigation, but one of the things that I wanted to—that I did point out earlier is that the greatest way to combat the loss of this information is to have an active security officer within each facility who talks to his people, who knows what is going on within that facility, who ensures the established safeguards for protecting the classified information are in effect—the Xerox machine is not used indiscriminately; access to that facility after hours is highly controlled. We must make sure that regular briefings are given to the employees. That is the best way to protect the security of that facility, even though you may have someone whose background cannot be checked out completely.

Senator **Nunn**. Obviously, background checks are important, or we wouldn't spent so much time and effort——

Mr. **Parker** [interposing]. Absolutely, but you also have to weigh what potential good can come from hiring that person with a particular skill; is that worth taking the risk that does exist.

Senator **Nunn**. I understand there are some very valuable people among this group, and I cast no general aspersions, but I think it points out a very, very significant problem, and you wonder whether 10,675—that magnitude—are necessary when you have that kind of defective procedure, not being able to investigate backgrounds.

So it is not the question of whether there ought to be any; it is the question of how many and how much risk can you take. That is an awful lot of people—almost 11,000 people on whom we have inadequate backgrounds.

I don't have an answer, but I hope we can get suggestions as the course of hearings go on. You generally got through with your testimony?

Mr. **Parker**. Yes, sir.

Senator **Nunn**. If I could go ahead and ask you questions here, in both the Harper and Boyce cases, classified documents were removed or copied after hours or on weekends. How important is some type of after-hours procedure to prevent access to facilities after hours?

Mr. **Parker**. I think you have just pointed out how important that is.

Senator **Nunn**. You say you don't have jurisdiction over that. That is not the FBI's job. Whose job is that?

Mr. **Parker**. That is the responsibility of the security officer within the facility who was following the rules as set forth by DOD.

Senator **Nunn**. How about in non-DOD facilities——

Mr. **Parker** [interposing]. Whichever agency is the contracting agency.

Senator **Nunn**. Do we have anybody who oversees it to see whether there are certain procedures in DOD and DOE that may be indicative of one doing a better job than the other? Is there any kind of umbrella look at the agencies?

Mr. **Parker**. I don't know, Senator.

Senator **Nunn**. Not that you know of?

Mr. **Parker**. I don't know of any organization such as that.

Senator **Nunn**. It is to each his own then as far as agencies?

Mr. **Parker**. There are certain requirements, insofar as handling classified material set out by DCI, which are to be followed concerning the type of safe, the access and the like.

Senator **Nunn**. Could you tell us, Mr. Parker, just in general the problems of the Veliotis case? Can you discuss that at all? We asked a series of questions of the FBI, I believe, about a month ago and have gotten no response on that case. What we are asking about is not a pending investigation; we are asking about the background checks that took place some years ago.

Mr. **Parker**. Senator Nunn, I am not at liberty to discuss that case.

Senator **Nunn**. Could you furnish for the record the answers to those questions? We have had DOE and DOD reveal the background checks that were made and all of the information they have on him. We don't have an answer as to why the FBI will not.

Mr. **Parker**. It is my understanding—I was not involved in the original discussions on the case—that various staffers and personnel from the FBI and the Department of Justice have discussed the matter, and it is the opinion of the FBI and DOJ that it would be better not to open this file at this time.

Senator **Nunn**. We have gotten access from the other agencies. I would like somebody to let me know, I can appreciate not in open session, I would like to know the reasons for that.

Mr. **Parker**. Yes, sir.

Senator **Nunn**. Again, I am not asking for current information. I am asking for really the background. We are not investigating the Veliotis case currently. We are looking at what went wrong with anything in the background.

Mr. **Parker**. Senator Nunn, I would certainly look into it.

Senator **Nunn**. I would appreciate it. We have a series of other questions, Mr. Parker, I would like to submit to you for the record. We appreciate very much you being here. We may have to call on you again as we formulate our conclusions and recommendations. You have been helpful this morning, and we thank you for that.

Our hearing tomorrow, contrary to the original notice, will begin at 9 rather than 9:30. We are trying to accommodate conflicts with various Senator's schedules, relative to both Senator Roth and myself and others are involved in.

Our first witness tomorrow morning at 9 o'clock will be Donald Devine, the head of Office of Personnel Management, and then we will follow with the testimony of Mr. Lawrence Howe and Mr. Eli Flyer. Both have gone into a great deal of detail and will have certain recommendations, and we will hear from the Department of

Energy as well as the Department of Defense, Assistant General Counsel.

Do you have any other observations, Mr. Parker? Any suggestions, anything you think we need to consider legislatively from the FBI point of view?

Mr. PARKER. Not at this moment, Senator Nunn. Thank you.

Senator NUNN. We will keep an open ear if you have suggestions because we will be making recommendations. Thank you for being here.

[Mr. Parker's prepared statement, with an attachment, and responses to written questions follow:]

PREPARED STATEMENT OF PHILLIP A. PARKER

There are approximately 2584 communist country officials assigned to Soviet, Soviet Bloc, and Cuban diplomatic and commercial facilities in the United States. Approximately thirty (30%) of these individuals are known or suspected of working actively in the United States for their country's intelligence services.

Probably the greatest achievement an intelligence service can have is the recruitment of an agent in a national defense related facility, or the penetration of private institutions where national defense related research and development work is performed. Recruited agents who do not have access to classified material or embargoed technology can be used as "spotters," who can supply personal data and access to persons who work with target material.

We welcome the opportunity to speak with you today about the government or government contract employee with access to classified or other sensitive data who commits espionage.

Safeguarding classified or otherwise sensitive information is a very difficult but most essential responsibility. When one considers the many areas in which research and development generate sensitive information, it is apparent that hostile intelligence services have a wealth of material available to them.

The collection mission of hostile intelligence service officers in the United States centers on the assessment and recruitment of Americans as agents. Hostile services are constantly in contact with Americans and are evaluating them as potential recruitment targets. If an American appears to have potential for development as an agent, several techniques or approaches may be used to recruit him. Above all, the development process is gradual, carefully planned and non-threatening in the early stages, and overall, is structured to exploit whatever weakness is detected and place the person in a position from which he believes he cannot extricate himself.

The methods employed to obtain sensitive information vary. Hostile services are eager to accept information offered by the disgruntled or mentally disturbed employee who may visit a hostile foreign consulate or mission in the United States, or abroad. They are aggressive in searching for and recruiting Americans at sensitive U.S. facilities, or taking advantage of persons with access to such facilities. They take advantage of the U.S. emigre population, especially those persons who have access to sensitive information and who may have relatives still residing in their country of origin. Commercial establishments in the United States serve as excellent cover mechanisms for intelligence collection.

Money and revenge may be characterized as two basic motivators of people who choose to commit espionage. Others may be drawn into espionage believing they are serving a cause other than that which is actually represented (false flag); still others find themselves in a situation where relatives abroad face uncertain futures without the cooperation of the person under recruitment. There are variations of these characteristics, but we usually find espionage springing from financial difficulties, greed, or professional and personal problems. In varying degrees, many of these problems may be detected and resolved before a person commits himself or herself to espionage.

Representatives of the Intelligence Division discussed with your staff a number of cases where classified or sensitive information was obtained by hostile intelligence services. I have with me today for the record summaries of these cases and others that I believe illustrate clearly the methods used by the hostile services. You will see from these summaries that our adversaries have any number of factors working for them in their collection programs. There are many reasons why a person chooses to commit espionage, and I think, these summaries show the basic motivation of these people. More important, I think these cases show the difficulty we face in detecting and countering this intelligence activity.

CASE SUMMARIES

William Holden Bell, a Hughes Aircraft project manager, sold classified information to a Polish intelligence service officer, allegedly to resolve financial difficulties.

James Harper used contacts with a Silicon Valley government contract facility to obtain classified material which he subsequently sold to the Polish intelligence services--his motivation, allegedly financial gain.

William Peter Kampiles committed espionage because his employer, the CIA, failed to recognize the view that he should be an agency case officer, although his work performance was unsatisfactory.

Edwin Moore, a CIA employee for 17 years, smuggled classified documents to his home and offered them for sale to the Soviet Union. Financial gain and revenge were factors which appear significant in this case.

Andrew Lee and Christopher Boyce committed espionage for a number of reasons, the principal being money, perceived political dissatisfaction and drugs.

Ronald Lou Humphrey chose espionage as the way to extricate his common-law wife and her children from Vietnman.

Financial distress apparently drove Joseph Helmich to commit espionage.

Thomas Patrick Cavanagh, a Northrup Corporation employee, attempted to sell classified information to persons he believed to be Soviet agents--for cash.

...and so on.

- - - - - - - - -

Each government agency or contractor must have a specific official responsible for security matters. This individual should be recognized as an ally and not an adversary, and the officer must have the training and time to perform his duties. Even in those cases where an intelligence officer has developed a social relationship, or pried loose some information, the Security Officer's job is to minimize the damage, protect employees from getting further ensnarled, and extricate the employee without further loss. If the employee remains silent, or does not know which way to turn, serious damage can occur. If fellow employees, knowing of a situation which might have compromised a fellow employee, remain silent, damage is almost certain. It is far better to have a suspected relationship voluntarily revealed, than to have this come to light in the course of an investigation, after damage has occurred.

There are a number of steps we might take to minimize the threat to our security through unauthorized acquisition of sensitive material.

If an employee or defense contractor has dealings with representatives of a foreign country, the most important step is to have all such contacts, including all foreign travel, reported to the Security Officer. At a minimum the Security Officer can monitor the contacts and insure a more effective inspection process where appropriate.

Through inspection process, the Security Officer should recognize when an association evolves from one of strictly business (or social) to one of a more personal nature. In recruitment scenarios, a key first step taken by intelligence officers is the development of a personal rapport and social relationship with targeted individuals.

We strongly endorse a system that improves physical security of facilities including controlled access areas, document accountability procedures, and "after hour" access approval.

The problem of safeguarding classified and sensitive material falls most heavily on the Security Officer. Security's role must be stressed, because the Security Officer and his staff face a broad front threat: from intelligence officers and their agents residing in the United States; from visiting commerical, scientific and technical delegations; from the hostile country emigrant population in this country; and from the mentally disturbed or disgruntled employee who strikes on the spur of the moment.

Other steps can be taken to minimize loss once espionage is detected; but more protection may be given long before the act of espionage. I am referring to the pre-employment background investigation, periodic up-date agency checks, and strong facility security programs, which include regular briefings.

BACKGROUND INVESTIGATIONS ON FBI-EMPLOYEES

The Administrative Services Division (ASD) is responsible for the hiring of all FBI personnel and, because of the large number of applicants versus the limited number of vacancies, this is accomplished on a highly selective basis. The application process for each applicant appointed is lengthy, detailed, and centers around testing, a personal interview, and an exhaustive background investigation that must meet requirements to grant a security clearance up to and including the Government's Top Secret level. Results of all these items are carefully scrutinized by case analysts and two to three levels of Special Agent supervisory personnel before an appointment is issued. In situations of admitted or developed contacts or relations with individuals in foreign countries, records of the Central Intelligence Agency are checked, the case results are evaluated by the FBI's Security Programs Office, and if deemed necessary, the applicant may be required to be interviewed by a foreign counterintelligence-trained Agent and possibly even undergo a polygraph examination. A polygraph examination may also be required in other types of situations in order to resolve questionable items discovered in the background investigation.

The FBI's application form, which all applicants must complete, is extremely detailed and covers all phases of a person's life. The applicant must undergo a personal interview in which all of the items on the application are reviewed and questioned. Following this, indices (internal records check) are checked on applicant and all listed individuals on the form. Background investigation is initiated on those selected for further processing. All information known at this point is verified and individuals are personally interviewed at all listed employments, schools attended, and at the last five years or residences, all with an eye toward disclosing the applicant's character, associates, reputation, loyalty, skills, and any other factor(s) reflecting on his/her suitability for the position sought from a security and skills standpoint. Any new or questionable information developed during the investigation is fully explored and resolved, if possible, during the investigative process, and as stated above, may require additional interviews of the applicant or a polygraph examination.

BACKGROUND INVESTIGATIONS FOR OTHER AGENCIES

The Federal Employees Security Program, established by Executive Order 10450, serves as the basis for most employment investigations in the Federal service; the order also has direct provisions concerning the FBI. The names of potential Government employees are searched through records at FBIHQ, including the fingerprint files of the Identification Division. In addition, background investigations are conducted for a limited number of agencies when requested in writing. Those presently served by the FBI are the White House (including the National Security Council), the Department of Justice, the Department of Energy, the Administrative Office of the United States Courts, and certain congressional committees.

The investigation and file reviews are designed to develop any information which could reflect adversely on one's suitability for Government employment or for security clearance purposes. The FBI provides the fully developed facts, particularly in regard to unfavorable information or other areas of concern, to the client agencies who have the responsibility for making employment or access determinations. The FBI does not make a recommendation to those agencies for or against employment or clearance. Also, many agencies provide for periodic update investigations which afford an opportunity for a reexamination of a person's background and for the development of any information which could have an adverse impact on continued employment with the Government.

The investigation encompasses an individual's adult life from age 18 and includes inquiries concerning residences, education, employments, military service, credit and arrests. Interviews are conducted with present and former neighbors, co-workers, supervisors, professors, roommates, references, and associates in an effort to develop comments concerning the individual's suitability for Federal employment and/or access to classified information.

Although the same general scope is applied to each investigation, the background of an applicant is carefully analyzed in an effort to identify areas where particular emphasis, based on that person's unique history, should be placed. In this connection, attention would be directed toward Federal, state and local agencies where records could exist concerning the applicant. Similarly attempts would be made to identify competitors, clients, professional associates, etc., who would be in a position to provide knowledgeable comments about the applicant.

A careful review would also be made of FBI files for any relevant information. In cases involving presidential appointments requiring Senate confirmation, a canvass is also made of all FBI field offices for information about a nominee.

Because of the need to make prompt appointments and to fill vacant positions, these investigations are assigned deadlines for completion and, in many instances, very short time frames are involved. When extremely short deadlines are necessary, the difficulty of ensuring that a complete and thorough inquiry has been pursued is increased but by concentrating our resources we believe we have been able to meet the demands placed upon us.

Close liaison is maintained with client agencies to ensure they are provided with pertinent information on a timely basis as well as to develop a smooth flow of requests which will permit us to manage our resources in this area more effectively and efficiently. Continual discussions occur on what the needs of these agencies are and procedural modifications are frequently made in efforts to improve service. We have also developed a computerized system which permits us to manage and direct these cases in a more effective manner.

BACKGROUND INVESTIGATIONS ABROAD

The FBI has no authority to conduct background investigations abroad. Where such investigations require checking foreign police, domestic security or intelligence organization records our Legal Attaches through established channels request pertinent information. We must rely on whatever information is provided; we are not in a position to verify or otherwise confirm information provided by the host country.

To some degree, we may request clarifications and ask follow-up questions, but we are completely dependent on the extent to which the foreign service chooses to cooperate. I might add that we have for the most part completely satisfactory relationships with our counterparts in the western services.

APPENDIX: FBI TESTIMONY BEFORE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS.

Financial Distress/Greed

William Holden Bell/Marian Zacharski
James Durward Harper, Jr.
David Henry Barnett
Joseph George Helmich, Jr.
Thomas Patrick Cavanagh

Revenge/Professional Dissatisfaction

William Peter Kampiles
Edwin Gibbons Moore, II

Political Motivation

Andrew Daulton Lee/Christopher Boyce

Blackmail/Hostage Situation

Otto Attila Gilbert

"False Flag" Approaches

Sahag D. Dedeyan/Sarkis Paskalian

Exploitation of an Emotional Involvement

Ronald Louis Humphrey/David Truong

Appeal to National Pride

Financial Distress/Greed

William Holden Bell/Marian Zacharski

On June 24, 1981 William Holden Bell, an employee of the Hughes Aircraft Corporation (HAC), was confronted by FBI Special Agents with the fact that the FBI had determined he was a recruited agent of the Polish intelligence services (PIS); Bell confessed. In October, Bell pleaded guilty to one count of passing secret documents to a foreign power. On November 16, the PIS intelligence officer in the case, Marian Zacharski, former President of the Polish owned commercial company, Polamco, was convicted of espionage. On December 14, Zacharski was sentenced to life in prison; Bell was sentenced to eight years in prison.

The case was initiated when information was developed that the PIS had recruited as an agent an employee of the HAC with access to classified data of interest to the Poles and their Soviet allies. Further investigation isolated an individual, Bell, who was an employee of HAC with pertinent access and who had a close social relationship with a Polish national, named Marian Zacharski.

Subsequent investigation of Bell revealed that he held a position at HAC as project manager of an advanced dual-purpose weapons system; he therefore had excellent access to classified data. He had also made several trips to Western Europe, conceivably to be debriefed by his PIS handlers. After another trip to Europe in April, 1981, it was decided to attempt to bring the case to a conclusion by confronting Bell with what would be the interviews in which he confessed.

In debriefings, Bell disclosed the full details of his dealings with Zacharski. Bell had developed a social relationship with Zacharski in the latter part of 1977. In the course of this relationship, Bell revealed to Zacharski that he was having financial difficulties. Zacharski offered financial assistance to Bell in return for HAC documents. Bell jumped at the offer, initially supplying the Pole with unclassified documents. Bell realized, however, that even by supplying Zacharski with unclassified documents, he had compromised himself and eventually the Pole would request classified material. Inevitably, Zacharski did begin to request classified material, and Bell was only too capable of satisfying PIS requirements. Bell was paid well for his services: in the course of the operation, Bell received approximately $110,000 in cash and a number of gold coins valued at roughly $60,000.

James Durward Harper, Jr.

On May 14, 1984, James Durward Harper, Jr., a United States citizen, was sentenced to life imprisonment on charges of espionage. FBI investigation had discovered that over a two and one-half year period beginning in 1979, Harper delivered voluminous classified documents to officers of the Polish intelligence services (PIS) in Europe and in Mexico. Included in these documents was extremely sensitive information relating to the Minuteman Intercontinental Ballistic Missile and the ballistic missile research and development programs of the United States. For his services Harper was paid in excess of $250,000 by the PIS.

Although Harper held no security clearance, he used his contacts in the Silicon Valley area of California including his now deceased second wife, Ruby Louise Schuler, to gain access to classified and restricted material. Schuler was employed by Systems Control Inc., Palo Alto, California, a government contract facility where she performed secretarial and bookkeeping duties. In her position, she had routine access to classified material for her superior, but would have no need-to-know the substance of the material.

The Harper case was not without significant Soviet overtones. In fact, after one particularly large delivery of classified documents by Harper, a special team of approximately twenty KGB analysts and engineers was dispatched from Moscow to Warsaw to evaluate the authenticity of the stolen documents. The KGB specialists quickly pronounced the documents authentic and valuable. In recognition of this intelligence coup, commendations were presented to the officers involved in the case. One of the commendations was signed by the KGB chairman Yuriy Andropov.

During post-arrest interviews with Harper, it became painfully evident that his sole motivation for committing espionage was financial. Harper had no political agenda, and was most unsophisticated in the art of spying. On one return trip from Warsaw, after delivering classified documents to the Poles, Harper actually stuffed the U. S. dollars he had received as payment in the athletic tube socks he was wearing and in his running shoes. Yet despite his crudeness Harper clearly illustrated the relative ease with which classified material can be transmitted to hostile intelligence services.

David Henry Barnett

On January 8, 1981, David Henry Barnett was sentenced by a Federal district judge to serve 18 years in prison. Barnett, a former intelligence officer of the Central Intelligence Agency (CIA) had, in October of 1980, pleaded guilty to a one-count indictment of espionage. The case also provided further evidence of increasingly aggressive efforts of the SIS to penetrate the highest levels of the U. S. Government.

On March 18, 1980, David Henry Barnett, a CIA staff officer from 1963 to 1970, was interviewed by Special Agents of the FBI based on investigation indicating his involvement with the KGB.

Barnett admitted he had sought out the Soviets and was recruited by them in the fall of 1976. He further admitted he had numerous contacts with the Soviets since being recruited and had supplied them with a great deal of information, for which he was paid a total of approximately $92,000. The sole motivating factor in his becoming a Soviet agent was financial distress. Upon leaving the CIA in 1970, Barnett attempted to establish an import-export business in Indonesia; the business failed. According to Barnett, his primary mission was to penetrate the CIA, with Defense Intelligence Agency and the U. S. Department of State being secondary targets.

Barnett provided Soviet agents with details of the CIA operation in Indonesia, including an accounting of the information acquired by the CIA and uses made of it by the United States. He also revealed the names of 30 CIA intelligence officers as well as the identities of agents recruited by the CIA.

Joseph George Helmich, Jr.

Joseph George Helmich, Jr., was arrested by the FBI on July 15, 1981, following a series of interviews in which he admitted cooperation with the Soviets in the early 1960's. For a payment of $131,000, Helmich passed to the Soviets extremely sensitive and vital information relating to the KL-7 cryptographic system (which at that time, was widely used by the U. S. military), including rotors, key lists, maintenance and instruction manuals, etc.

In August, 1980, after a lengthy investigation, it was decided by the FBI to contact Helmich directly and confront him with an interview. During initial interviews of Helmich in August, 1980, he admitted that he first contacted the Soviets as early as 1962 and he had received $20,000 in payments from the Soviets; but he maintained that he had not compromised any classified information.

Eventually, Helmich recounted the full details of his espionage activities. Throughout his tour of duty in France, he had continual financial difficulties and in particular, was constantly being reprimanded for passing insufficient funds checks, at various military clubs. Finally, in early 1963, he was told by his commanding officer that unless he resolved approximately $500 to $700 worth of bad checks, he would be court-martialed. Unable to acquire a bank loan and faced with a one day deadline to pay his debt, Helmich decided to turn to the Soviets for financial assistance.

Helmich probably did not realize the full bartering value of the product he had at his disposal. He was assigned to a communications center which initiated, received, and relayed messages, handling everything from routine traffic to highly sensitive messages. As a Warrant Officer, Helmich was afforded all the necessary clearances and had access to all communications equipment including card keys and card blocks, keying lists, operations manuals, all cryptographic machines (specifically the KL-7 and KW-26), and spare parts.

With a sample of the type of information he had for sale, Helmich visited the Soviet Embassy in Paris and told the Soviets where he was assigned. Needless to say, the Soviets readily agreed to deal with him and a meeting was set up for the next day. For the next few weeks (Helmich was due shortly to be transferred to Ft. Bragg, North Carolina) he met with the Soviets on several occasions and provided them with a bounty of information relating to the KL-7 cryptographic system.

Upon being transferred to Ft. Bragg, Helmich continued to provide the Soviets photographs of KL-7 key lists, and to this end travelled to both France and Mexico City to rendezvous with SIS handlers. The value the Soviets placed upon the material was evident. Aside from paying Helmich roughly $131,000, Helmich was told that, due to his achievements, he had been promoted to the rank of Colonel in the Soviet Army and that he had been awarded a First Class Hero's Medal of the Highest Order.

On September 28, 1981, Joseph George Helmich, Jr., pleaded guilty to charges of conspiracy. On October 16, Helmich was sentenced to life in prison.

Thomas Patrick Cavanagh

On March 14, 1985, Thomas Patrick Cavanagh, who was formerly employed as an engineering specialist with the Northrop Corporation, Pico Rivera, California, pleaded guilty to two counts of espionage in violation of Title 18, U.S.C. Section 794 (a) (attempting to communicate and deliver classified documents to agents of a foreign power). Cavanagh had been arrested by Special Agents, in Commerce, California, after attempting to sell classified documents to Undercover Special Agents (UCAs).

This case originated when an individual was detected contacting the Soviets and offering to sell classified documents. A meeting was proposed in a Los Angeles motel, where a deal could be negotiated. Based upon this information on UCAs, posing as Soviet diplomats, met with the individual later identified as Cavanagh, at the prescribed location. At this meeting, Cavanagh asked for $25,000 in cash for classified information, and dispayed a sample of what he had to offer to the UCAs. A second meeting was arranged at which a full scale deal could be consummated.

The second meeting was held and a portion of highly classified documents were passed to UCAs. No money was exchanged, but Cavanagh was told that at the next meeting he would be paid $25,000 in cash per month over a ten-year period for additional classified information. At the third meeting, Cavanagh delivered more documents, for which he was paid $25,000. He was then arrested by Special Agents.

FURTHER COMMENT SHOULD BE WITHHELD AS CASE PENDING JUDICIAL ACTION.

Revenge/Professional Dissatisfaction

William Peter Kampiles

Some of the greatest intelligence coups have been the result of the efforts of an intelligence servi , but rather have come about as the result of a windfall Such was the path through which the Soviets acquired t "KH-11 System Technical Manual." The manual was sold the Soviets in February of 1978 by former CIA employe William Kampiles for a mere $3,000. The Top Secret document sold is a technical manual for an advanced American reconnaissance satellite.

The apprehension of Kampiles came about as a result of his own action. In a letter given to a former CIA colleague, Kampiles recounted how he had accidentally met a Soviet in Athens in February of 1978. Although Kampiles did not mention in the letter the actual sale of any material to the Soviets, he did describe more than one meeting with a Soviet, and did note that he had discussed such things as his access to classified material and the type of information the Soviet wanted.

Having thus drawn attention to his activities, Kampiles was soon thereafter contacted by FBI Special Agents. In an interview, Kampiles confessed to the act of espionage. He admitted that, while on a visit to Greece, he went to the Embassy of the Soviet Union, where he met a man whom he later determined to be Director of Security for the Embassy. In subsequent visits, Kampiles supplied the manual to the Soviets for the sum of $10,000, of which $7,000 was to be supplied at a later date.

Kampiles had obtained the document during his service as a GS 7 Watch Officer assigned to the CIA Deputy Director of Intelligence (DDI) Operations Center. He was employed in this capacity from March 29, through November 4, 1977, and in view of his sensitive duties with the CIA, held a large variety of security clearances.

Kampiles was motivated to a great extent by disgruntlement towards the CIA. He desired a transfer to the Directorate of Operations in CIA where he could become a case officer. Due to Kampiles' poor work performance, CIA officials considered this to be out of the question. Kampiles was told this in no uncertain terms. He was also sharply criticized for his unsatisfactory work performance. Soon after, Kampiles stole the KH-11 Manual. On December 22, 1978, he was sentenced to 40 years in prison.

Edwin Gibbons Moore II

During the evening of December 21, 1976, a Soviet security guard at a Washington, D. C., apartment house owned by the Soviet Union found a large, plastic wrapped, manila envelope on the building grounds. He notified an Executive Protective Service guard who notified the local U. S. Army Explosive Ordnance Detachment (EOD). The package was examined and found to contain several documents, apparently the property of CIA, and two notes requesting money. One of the notes also offered "penetration into the headquarters operation of the CIA" through the furnishing of a wide variety of documents while the other, addressed, "For Resident Eyes Only," contained instructions for two "drops" of money, totaling $200,000 to be made December 22, 1976. At about 2 p.m. on that date a Special Agent of the FBI "dropped" a dummy package as instructed.

Edwin Gibbons Moore, II, raking leaves at his home across the street from this drop site, was seen to make 5 trips past the drop site and package to a wooded field where he dumped the leaves. Returning from the 5th trip he stopped, placed his foot on the package, then picked it up. He was immediately arrested by the FBI.

Moore, 57, had been employed by the CIA from 1952 through May, 1963, and again from October, 1967, through June, 1973, when he retired on medical disability having held the grade GS-9 from 1954 until his retirement. Throughout his employment, Moore held a Top Secret clearance, and, from 1956 until 1961 a Special Intelligence clearance. Moore took full advantage of these clearances by smuggling classified CIA documents from his place of work and storing them in his home.

Although financial gain was a motivational factor spurring on Moore's attempt at espionage, it is probable that he was also very disgruntled with his former employer. He had been passed over for promotion many times in the course of his career and consequently remained frozen in his GS-9 slot. Furthermore, he had been involved in litigation with the CIA for a number of years (which accounts for his break in service).

Moore was convicted of a number of charges, including transmitting national defense information to a foreign power, and on December 8, 1977, was sentenced to 15 years in prison.

Political Motivation

Andrew Daulton Lee/Christopher John Boyce

In April, 1977 Christopher John Boyce was tried and convicted on charges of espionage. During the next month Andrew Daulton Lee was likewise tried and convicted of espionage. They were both sentenced to life in prison. Boyce, formerly an employee of TRW, Inc. had, in tandem with Lee (who served as a go-between) sold to the Soviets, for a total of approximately $70,000, a large amount of sensitive data relating to U. S. surveillance satellites. The loss represented a devastating blow to U. S. national security interests.

The activities of Andrew Daulton Lee and Christopher John Boyce came to the FBI's attention when Lee was arrested January 6, 1977, in Mexico City, by police on duty at the Soviet Embassy. He was observed throwing an object onto the Embassy grounds and while he was being questioned by the police officers, a U. S. Embassy employee, who was at the Soviet Embassy on official business, was asked by Lee for help in explaining himself to the police. A second Embassy official was notified of the situation and accompanied Lee to the police station where it was discovered Lee had an envelope containing a number of film strips. An examination disclosed the film was of documents bearing "Top Secret" markings. Mexican authorities subsequently delivered prints of the film to U. S. Embassy officials. It was determined the documents in question related to a U. S. Government project with a California-based space and defense communications company, TRW, Inc.

Questioning of Lee by Mexican security officers and FBI representatives in Mexico City resulted in Lee naming Boyce, an employee of TRW, as involved with Lee in what the latter described as a scheme to furnish the Soviet Union with outdated and worthless data in exchange for substantial payments.

Acting on Lee's information concerning Boyce, the latter was arrested on January 16, 1977 in California. Boyce acknowledged that he had given Lee data from TRW which he knew was being passed to the Soviets, but claimed that he had furnished only outdated and valueless information. Despite Lee and Boyce's claim that they had sold worthless data, they both were convicted on charges of espionage. In extensive debriefings which occurred after their convictions, they revealed in detail the extent of their dealings with the Soviets.

Although financial motivations definitely played an important part (particularly relative to Lee, who needed money to finance an expensive drug habit and business) in the Boyce/Lee case, there is also evidence that Boyce was also motivated by political dissatisfaction with the United States. Coming of age in the politically heated climate of the early 1970's, Boyce often spoke to his friends of his disgust with U. S. involvement in Viet Nam and with the Watergate scandals. In turning to espionage, Boyce was at least in part spurred on when he learned of CIA involvement in the internal politics of Australia. Lee received a life sentence, while Boyce received 40 years plus 25 years on the escape charge.

Blackmail/Hostage Situation

Hostile intelligence services can play rough in their drive to compromise and recruit U. S. citizens when Americans are visiting communist countries. Attempts at compromising Americans through sex and other ploys, while they are touring the Soviet Union and other East European countries, are not at all uncommon. At the same time, it should be emphasized that this approach is seldom, if ever, employed within the United States (although knowledge of any personal vulnerabilities of Americans is sought in the United States for exploitation abroad).

Otto Attila Gilbert

Another tactic employed by the hostile intelligence services is the exploitation of hostage situations. If a foreign intelligence service learns that a targeted individual has relatives in Eastern Europe, the USSR, Cuba or the People's Republic of China, the individual is regarded as being in a potentially vulnerable position. First will come gentle persuasion. An intelligence officer may produce "letters" from relatives calling for an American to "cooperate." If that does not work, the intelligence officer may suggest that harsh measures could be applied to the relatives. There is no easy answer to the American who finds himself approached in this manner, because the ability of the hostile intelligence service to apply pressure through the target's family is unquestionable.

One case in which a hostage situation potentially existed fortuitously developed into an FBI DA operation which culminated with the arrest and conviction, on charges of espionage, of Otto Attila Gilbert, an agent of the Hungarian intelligence services (HIS).

The origins of the operation date back to December, 1977, when a naturalized citizen of the United States, a U. S. Army serviceman of Hungarian descent was approached, while visiting family members in Hungary, by an individual who was later identified as a known intelligence officer (IO) of the HIS. The serviceman was requested to obtain information on U. S. and North Atlantic Treaty Organization (NATO) military forces, and was informed that Hungarian authorities had conducted extensive investigations into the background of his family and determined that it consisted, in general, of individuals who were loyal to the Hungarian

Communist Party. The IO also noted that although the serviceman, a military policeman, had committed no outright crime, there were certain irregularities associated with the nature of his visit to Hungary.

After this ominous comment, the IO added that if the serviceman cooperated, future visits to Hungary would be assured and his mother would in turn be allowed to depart Hungary for visits to the U. S. If information supplied to the IO was deemed to be of sufficient value, he would be willing to pay for the data. The serviceman replied that he would have to mull over the offer, and the IO gave him a telephone number through which the IO could be contacted, as well as some preliminary taskings. Shortly thereafter, the serviceman departed Hungary.

Although the IO had levelled a threat, if ever so subtle, against both the serviceman and his relatives in Hungary, the serviceman nevertheless reported the contact upon return to his base in West Germany. A double agent (DA) operation was then initiated by the U. S. Army. After several meetings with the HIS in Europe, the serviceman was transferred to the United States, and the operation then became a joint U. S. Army/FBI endeavor.

Following a number of meetings in Europe, in which the DA passed authorized material to the HIS, the Hungarians were encouraged to arrange a meeting in the United States, counter to standard HIS modus operandi.

Apparently believing in the credibility of the DA, the HIS indeed agreed to dispatch a courier to pick up the material on a specified date in Augusta, Georgia.

On April 17, 1982, the HIS agent approached the DA at a predetermined meet site. The DA and an individual later identified as Otto Attila Gilbert reviewed the classified documents, Gilbert choosing which ones to accept. Gilbert paid $4,000 in cash for the documents. Upon exiting the vehicle, Gilbert was arrested. He was indicted by a Federal grand jury on charges of espionage. He was convicted of those charges in August, 1982 and received a sentence of 15 years in prison.

"False Flag" Approaches

Sahag D. Dedeyan/Sarkis Paskalian

In another maneuver, a hostile intelligence officer misrepresents himself as a citizen of a country friendly to the United States. The is called a false flag approach. Thus, a targeted American may be duped into handing over sensitive information by being led to believe that he is aiding an ally of the United States. In a variation of this tactic, an intelligence officer or a hostile intelligence service agent poses as a representative of a noncommunist country or entity, towards which a targeted American is particularly sympathetic.

This approach was used during the mid-1970's in a case involving Sahag Dedeyan and Sarkis Paskalian. Dedeyan, who is a naturalized U. S. citizen of Armenian extraction and who was employed by Operations Research Incorporated, Silver Springs, Maryland, was approached by Paskalian, who said that he was a distant relative. Paskalian claimed he was working for Armenia, with the assistance of the Soviet Union, in a drive to reclaim lost Armenian lands from Turkey. In actuality, Paskalian was a KGB agent.

Paskalian developed the friendship so that eventually he became a regular guest at the Dedeyan home. Dedeyan, in his capacity at Operations Research, had access to classified data, and during one visit Paskalian surreptitiously photographed a "Secret" document which Dedeyan had stored in his home. Several months later, Paskalian admitted that he had photographed the document and offered Dedeyan $1,000 in cash to maintain silence. Dedeyan accepted the payment.

Shortly thereafter, both individuals were arrested. Paskalian was indicted on espionage, convicted, and sentenced to 22 years in prison. Dedeyan was indicted on charges of failure to report the abstraction of a national defense document, and convicted of those charges. He received a sentence of three years in prison.

Exploitation of an Emotional Involvement

Ronald Louis Humphrey/David Truong

On May 20, 1978, an Alexandria, Va., federal court jury returned a verdict of guilty in the espionage trial of the United States of America vs. Ronald Louis Humphrey and Truong Dinh Hung, aka David Truong. The defendants were found guilty of six of the seven counts in the indictment, which related to violation of the espionage and similar statutes (they were found not guilty of count six, which pertained to receiving stolen property). The trial arose out of the alleged passage of material "relating to the national defense of the United States" to the Socialist Republic of Vietnam (SRV). Several weeks later, on July 15, the two subjects were each sentenced to 15 years in prison.

This Vietnamese intelligence operation consisted essentially of the transmittal of classified U. S. Department of State documents by Humphrey and Truong to representatives of the SRV. The material, which was composed of both "Secret" and "Confidential" documents, included, but was not limited to, information concerning United States political, military, and diplomatic relations, efforts, and intelligence assessments in Thailand, Singapore, Vietnam, the PRC, and Ethiopia. During 1977, the United States and the SRV were involved in negotiations, and much of the purloined information could have been of value to the Vietnamese in establishing a bargaining position vis-a-vis the Americans. Humphrey, who held a "Top Secret" security clearance, had access to the information due to his status as a Foreign Service Information Officer with the United States Information Agency (USIA), in which capacity he was charged with the task of monitoring foreign cable traffic at USIA headquarters.

Humphrey was motivated to act as an agent for the SRV by his desire to gain the release of his common-law wife from Vietnam. Humphrey met her in 1969 while serving in Vietnam, and developed an intense relationship with the woman. She followed Humphrey when he was assigned to Germany, although she was forced to leave two offspring behind in South Vietnam. She returned to Saigon in April of 1975 in an attempt to extricate her family, but became stranded there when South Vietnam fell to the North Vietnamese-Viet Cong onslaught.

Appeal to National Pride

A common ploy used by hostile intelligence services against the immigrant community in the United States, is an appeal to an individual's national pride. An immigrant will be encouraged by an intelligence officer (IO) posing as a diplomat, to perform services for his native land, whereas in reality, the unsuspecting immigrant is being recruited by the intelligence service. This recruitment ploy was well illustrated in what, fortuitously, evolved into an FBI double agent operation aimed against an East European intelligence service and resulted eventually in the expulsion of an IO.

The origins of this case extend back to mid-1970 when an individual of East European descent, employed by a major U. S. computer firm, was visiting his native land at the invitation of that country's Government. The individual was, of course, graciously treated; he and his wife were assigned a female "guide" to accompany them on their tour. Intriguingly, the "guide" mentioned to the tourists that her "son" wanted to become a computer programmer, and requested that the visiting computer specialist send her some information on computers. Upon returning to the United States, the individual duly complied, sending the "guide" some very basic information relating to computers. Of course, in all probability, the "guide" was in reality a spotter for the East European country's intelligence service, whose assignment was to assess the emigre's potential as an agent.

The intelligence service apparently made a positive assessment of the emigre's potential, for one year later, he was contacted by a known IO assigned to a Consulate in New York City. The IO set up a luncheon date with the emigre. Recognizing that this was a highly unusual incident, the emigre immediately contacted the FBI, where his cooperation was enlisted. The IO began to negotiate for the acquisition of more computer-related data, stating that the emigre could "be an official advisor to his native land on computers." As a recruitment ploy, the IO argued that the asset's assistance to his native land would be comparable to the institution of the Marshall plan by the United States Government after World War II.

RESPONSES TO WRITTEN QUESTIONS

Question 1. Where do you feel our personnel security system is most vulnerable to hostile intelligence force activities?

Answer. We believe hostile intelligence services are able to exploit our personnel security system for several reasons: lack of periodic update or reinvestigation of national agency checks; inadequate controls on after hours or unauthorized access to classified or sensitive information; and insufficient controls on documenting of contacts with foreign nationals, or travel abroad.

Question 2. You have mentioned the increase in the number of espionage cases currently pending in our courts. Do you feel this is indicative of anything? Is it just better law enforcement or is it indicative of a defect in our personnel security system that is now coming to light?

Answer. In large part, we see an increase in the number of espionage cases in the courts as a result of our increasingly sophisticated investigative techniques, improved and closer cooperation and coordination with other government agencies, and increased used of counterintelligence awareness programs. We see no diminishing of the threat.

Question 3. Can you suggest any improvements in our personnel security system to respond to the hostile intelligence that you have described to us?

Answer. We believe that periodic updated investigations, strengthened controls on access to classified or sensitive information, and mandatory controls on reporting contacts with foreign nationals and travel abroad are necessary. We should strive for consistency in background investigations by the various government agencies. And we should emphasize counterintelligence awareness programs.

Question 4. You have detailed in your written statement the procedures used by the FBI to approve your own employees. Do you know how your methods differ from those of the Office of Personnel Management (OPM) or Defense Investigative Service (DIS)? If so, how so?

Answer. We do not have sufficient information regarding the methods used by OPM or DIS to adjudicate their own background investigations in order to compare those methods with our own. We have submitted in our written statement an extremely detailed explanation of our adjudication system. We would suggest that the Subcommittee obtain from both OPM and DIS the methods used by them to approve their employees in order to compare that information with the information contained in our opening statement.

Question 5. Do you agree with the conclusion of the December 1984 DOD Industrial Security Review Committee Report that the weakest link in our personnel security system is the secret clearance since it is based upon an NAC, alone, with no periodic update? What would you recommend in its place?

Answer. A national agency check without periodic update is inadequate. We recommend the NAC include updated investigations.

Question 6. What is your opinion about the same Committee's recommendation that all foreign travel by contractor employees be reported to DIS? How would this be helpful to your agency.

Answer. We strongly endorse reporting of all foreign travel and contact with foreign nationals. Security authorities including the Defense Investigative Service must be alert to hostile intelligence service activities. This reporting is helpful to the FBI and offers us an opportunity to monitor possible hostile recruitment efforts.

Question 7. As you are aware, both OPM and DIS have been severely hampered in obtaining criminal records from state and local agencies due to their ambiguous law enforcement status. Do you feel this is a problem? Would you support such a clarification solely for the purpose of enhancing their ability to collect criminal records?

Answer. Yes, it is a problem. Under Title 28, United States Code, Section 534, both OPM and DIS are furnished with all criminal history records on file in the FBI Identification Division. However, Federal regulations (Title 28, Code of Federal Regulations, Section 20.1—20.36) are being interpreted by some states to deny OPM and DIS access to criminal history records. This is partly because of ambiguities in the regulations and because OPM does not meet the regulations' definition of a criminal justice agency nor is the purpose for which it wishes to obtain records clearly authorized by the regulations. Clearly, OPM is not a criminal justice agency, therefore, the answer is to expand the purposes for which criminal records can be used. Eliminate the ambiguity in the regulations. Make it clear that these records are available to Federal noncriminal justice agencies for the employment and security checks required by Executive Order. The FBI Identification Division would support such a clarification to enhance the ability of OPM and DIS to collect criminal history records.

Question 8. Both OPM and DIS have a similar problem in gaining access to records due to their not having a National Crime Information Center number (NCIC). Do you agree with their position? Would you support their attempts to obtain an NCIC number?

Answer. Fourteen DIS Regional Offices have NCIC Originating Agency Identifiers (ORIs) assigned. These unique numbers are assigned as a control to ensure that only criminal justice agencies engaged in the administration of criminal justice as defined by 28 CFR 20.3 and NCIC policy are granted terminal access to NCIC records. Although OPM does not meet this definition, a unique FBI Identification Division (ID) number has been assigned for its access to ID records. The absence of the NCIC number would not preclude the receipt of NCIC records off line, however, if statutory authority to access records is present.

The issue as presented in the question appears to be that both agencies have had difficulty obtaining access to records from state data bases. State law and their policies control granting access to state records, however, states may on occasion equate the possession of an NCIC ORI with the right to access state records. The FBI in no way controls access to these state records. OPM and DIS have recently participated in an FBI sponsored Federal Agency meeting to address problems being encountered in the states and to identify possible solutions to obtaining state criminal history records.

Question 9. Are all of the FBI investigative files included in your general indicies? It is our understanding that 40–50-percent of your criminal investigative files are not included in them. Thus, the usual National Agency Check you do does not include the check of these files.

Answer. The Office of Personnel Management defines a National Agency Check (NAC) as a check that consists of record searches with selected sources covering specific areas of the subject's background. One such record search is a review of the subject's name and aliases through the FBI's Central Records System (CRS) located at FBI headquarters (FBIHQ). The CRS is the repository of all pertinent, relevant information that is developed by FBI field offices and forwarded to FBIHQ. The CRS also contains all correspondence received directly at FBIHQ from non-FBI sources, i.e., other Federal and local agencies, private citizens, etc. During the processing of a record search in connection with the NAC, any information contained in FBIHQ files that is not complete or requires further clarification is resolved by communicating with the appropriate field office for an update or a final resolution of the matter. Certain information developed by field offices is not reported to FBIHQ. Examples include, but are not limited to, cases related to matters where no FBI jurisdiction is indicated or the complaint proves to be unfounded. The FBI is in the process of automating its CRS. This initiative provides for source data entry of index information by all field offices, thereby assuring that field office data currently not forwarded to FBIHQ will be retrievable in the future for record searches conducted pursuant to the NAC.

Question 10. Additionally, another potential loophole in the National Agency Check concerns the fact that your general indices do not include the investigative files of all federal law enforcement. This isn't a criticism of the FBI but rather of those agencies who are utilizing a general indices or FBI fingerprint identification checks as the sole check of all law enforcement files. Would you please comment on this.

Answer. The Central Records System (CRS) maintained at FBIHQ does not contain complete investigative information from all Federal law enforcement agencies. Other Federal law enforcement agencies, such as the Drug Enforcement Administration, the Immigration and Naturalization Service, the U.S. Border Patrol, the Bureau of Alcohol, Tobacco and Firearms, the U.S. Secret Service, have in many cases exclusive jurisdiction over certain investigative matters. These agencies generally do not provide the FBI with investigative information for inclusion in the CRS at FBIHQ. In addition, the various Inspectors General in the Executive Branch conduct investigations which are not reported to FBIHQ and included in the CRS. However, the definition of an NAC promulgated by the Office of Personnel Management indicates that a NAC consists of record searches with selected sources covering specific areas of the subject's background. Should the Office of Personnel Management of other Federal agency initiating a NAC have reason to believe that one or the other previouly-mentioned Federal law enforcement agencies or Inspectors General might have compiled investigative information on the subject, a request for a review of that agency's records may be made independent of the search of the CRS at FBIHQ.

The FBI Identification Division was established by specific congressional enactment and is designated as the central repository for fingerprints and related identification data submitted voluntarily by law enforcement and other authorized governmental agencies. As noted, the law does not require law enforcement agencies to submit their arrest data to the FBI Identification Division. All data on file in the FBI Identification Division is supported by the individual's fingerprints. Since February 1973, the FBI Identification Division has not stored nonserious arrest charges as defined in Title 28, Code of Federal Regulations, Section 20.32, in its system. The FBI Identification Division is aware of only one major police department (Metropolitan Police Department, Washington, D.C.) that does not routinely forward their arrest fingerprint cards for serious offenses for filing. However, since the system is a voluntary one which does not contain nonserious charge data, not all arrest information can be obtained by merely checking the Criminal File of the FBI Identification Division.

Question 11. Does every police department report their cases to the FBI? When you check your indices for, let's say OPM or DIS, do you assure them that they will pick up these missing local agency files?

Answer. No law requires that all arrest data be forwarded to the FBI Identification Division. It is a voluntary system that currently contains arrest data on over 22 million individuals. Only one major police department, i.e., the Metropolitan Police Department in Washington, D.C., does not routinely forward arrest fingerprint cards to the FBI. OPM, DIS, and other authorized governmental agencies checking the Criminal File of the FBI Identification Division are aware of the limitations of our data base. We do not assure them that our Criminal File contains all arrest data. We encourage them to check arrest records at both the state and local levels.

Question 12. It is our understanding that there has been a recommendation made by the Board of Governors of NCIC that henceforth only the first arrest will be reported to NCIC, all records of subsequent arrests will be maintained by the states. Will this negatively impact on OPM's background investigations for Secret clearances?

Answer. The NCIC Advisory Policy Board has not made a recommendation that only the first arrest will be reported to NCIC. The FBI was requested to test a decentralized record keeping concept as an alternative to the current centralized Identification Division (ID) record data base. The concept recently tested is known as the Interstate Identification Index (III). Two phases of testing have been successful. This system envisions the FBI continuing to provide fingerprint services and identification functions; the continuation of a record repository for Federal arrest and disposition data; and the management of an index of personal descriptive data, unique identifiers, and the identity of the state(s) where the arrest and disposition data is maintained. the index is now composed of over nine million records, 4.2 million of which 17 states have assumed decentralized responsibility for the record keeping. The ultimate stage of the III, a National Fingerprint File, would eliminate the duplication of record keeping at the Federal level when records are maintained at the state level. The FBI is currently studying the opportunities and obstacles in noncriminal justice agencies obtaining access to criminal history records from the states holding the records. Until such time as a system can be devised to accommodate legally authorized noncriminal justice criminal history record checks, the record services of ID will be continued. Although the submission of arrest and disposition data from the states is voluntary, all states have been encouraged to continue their present practice of submission of records to the ID until an alternative record delivery service can be established. Any system designed would necessarily provide for criminal history record checks to support Secret clearances.

Question 13. (a) Would you please furnish us with a list of companies operating within the U.S. that are owned or controlled by a communist or communist-bloc country,

(b) Do you provide this list to contractors under the DECA program? If not, why not?

Answer. The List of communist bloc commercial companies operating in the United States is classified and cannot be provided for publication in an unclassified format. This list has been furnished to the U.S. export control community, including the Pentagon, the Department of Commerce, U.S. Secret Service, the Department of Justice, and the Defense Industrial Security Clearance Office. The list has not been furnished to contractors under the Development of Counterintelligence Awareness (DECA) program; however, these facilities are made aware in our contacts of the use of such firms for intelligence-related activity. In addition, most of the firms on the list are engaged in legitimate commerce, and we believe wide dissemination might result in inaccurate inferences with regard to those firms where no information is available indicating their use by hostile intelligence services.

Question 14. Since the FBI has no authority to require government agencies to conduct periodic update background investigations, what recommendations would the FBI make to assure consistency in this area?

Answer. Periodic updates are a valuable means of identifying potential sercurity-related problems. Requirements are set forth in the Federal Personnel Manual and Director of Central Intelligence Directive No.1/14 concerning periodic updates by agencies can apply them in differing degrees.

One common difficulty often cited in connection with periodic updates is a lack of adequate resources. We would recommend that sufficient resources be available to agencies overall to operate an effective personnel security program which would include periodic updates.

Standardization of procedures within the Executive Branch would help improve consistency in this area.

Question 15. As you are aware, both OPM and DIS have been severely hampered in obtaining criminal records from state and local agencies due to their ambiguous law enforcement status. Do you feel this is a problem? Would you support such a clarification solely for purpose of enhancing their ability to collect criminal records?

Answer. Since a check of criminal records is a fundamental part of any suitability or security consideration, an effort to clarify the saw enforcement nature of background investigations in order to encourage state and local agencies to provide greater access to these records would be helpful.

Question 16. On March 11, 1985, the Subcommittee staff met with officials of the Justice Department and the FBI in the hope of obtaining information about Takis Veliotis's personnel security investigations conducted by the FBI at the request of the Department of Energy in 1977. The Justice Department and FBI officials refused to reveal any information about the investigation. In anticipation of the FBI's participation in these hearings, the Subcommittee turned over a series of questions which are aimed at obtaining information about the Veliotis inquiry. I would like to have an explanation why the FBI has been unwilling to provide this information to the Untied States Senate. Please explain why you have refused to cooperate with this portion of the investigation.

Answer. As your subcommittee has been previously informed, the Department of Justice is pursuing an active criminal investigation involving Mr. Veliotis and has determined that no information from FBI or Department of Justice records can be released at this time.

Question 17. In a letter signed by me as Ranking Minority Member, we have asked the FBI for its files on the background investigation on Panagiotis Veliotis. To date, we have received no response to this request; nor has the Bureau turned over the files to us. Both the Department of Energy and the Department of Defense have provided us their files on the clearance investigations on Veliotis. Both departments have testified about this matter and answered all questions posed by the Subcommittee during our recent hearings. In light of the full cooperation on those two agencies, has the Bureau reconsidered its position on our request? If not, why not? Please explain in detail.

Answer. See response to preceding question.

Question 18. In the 1977 inquiry, according to Energy Department records, the FBI noted that Veliotis had been convicted of money order fraud in the Court of Misdemeanor in Piraeus, Greece in 1954 and received a 45-day sentence. Can you tell us more information about this reported conviction?

Answer. The only information available to the FBI is information provided by the Regional Security Office, U.S. Embassy, Athens, Greece, that Greek criminal records disclosed Mr. Veliotis received a sentence to 45 days imprisonment, in accordance with Decision #10 of June 7, 1954, of the Piraeus Court of Misdemeanors for the issuance of "uncovered money orders."

Question 19. (a) What is the policy of the FBI's counterintelligence section when it is determined that a senior defense industry official—an executive with top secret clearances—might have been involved in fraud? This is what happened in 1982 when the Justice Department decided to include Veliotis as a subject of a grand jury probe in the Southern District of New York. Was the counterintelligence section advised that Veliotis might have been involved in a million-dollar kickback scheme?Is this the kind of information that the Bureau should have on a timely basis?

(b) On February 5, 1982, federal prosecutors from the Southern District of New York informed General Dynamics that Veliotis was a subject in a federal grand jury. Mr. Veliotis was in managerial positions overseeing the Quincy and Groton yards, both of which have top secret facility clearances and highly sensitive military and nuclear propulsion programs. Are you aware of any information from Justice conveyed to the FBI' counterintelligence unit on the possibility that Veliotis was under grand jury investigation? Do you think a procedure should be in place to convey information of that nature?

(c) General Dynamics officials have told the Subcommittee that on February 5, 1982, a federal prosecutor in the Southern District of New York, David Denton, told General Dynamics officials that Veliotis was a subject in the grand jury probe of alleged Fringitemp kickbacks. Was the counterintelligence section of the Bureau also advised? Would it have been appropriate to put the counterintelligence people on notice that a man with a top secret clearance and a "Q" access authorization and a man with access to top secret naval nuclear propulsion information was suspected of possible wrongdoing?

Answer. These three questions address similar issues. Normally information is not referred to the counterintelligence component of the FBI unless there is a clear allegation the individual is involved in activity, such as espionage, which is inimical to national security interests. However, when information is developed that a person employed at a vital facility is engaged in criminal conduct, it is important that the agency with responsibility for the facility (which presumably grants the security clearances) be informed by the agency developing the information. The FBI does have general instructions that, when such information is developed concerning aperson employed at, or having access to, a vital facility, dissemination to interested agencies should be made. In connect with this matter, the FBI did not become involved in the criminal investigation of Mr. Veliotis until 1983. He had left General Dynamics in 1982.

Question 20. (a) Did the FBI conduct the investigative work on behalf of the Energy Department in connection with the application of Panagiotis Takis Veliotis for a "Q" access authorization in 1977?

(b) What are the normal procedures which are followed when the Energy Department requests the FBI to do such a background inquiry?

Answer. On August 11, 1977, the FBI received a request from the Energy Research and Development Agency (ERDA) (predecessor of the Department of Energy) to conduct a background investigation on Panagiotis Takis Veliotis in connection with his employment with General Dynamics Corporation where he would have access to restricted data and exclusion areas. Based on this request a full-field investigation was initiated which included interviews with employers, neighbors, references, and associates as well as credit and criminal checks and record checks of logical federal agencies as well as checks of records at FBI Headquarters and in pertinent field offices. In addition, FBI representatives abroad were requested to conduct logical inquiries in Canada and Greece. The full results of the completed investigation were transmitted to ERDA on September 20, 1977.

Question 21. In connection with this case, Veliotis was born in Greece and a citizen of both Greece an Canada. A situation like this does not come along too often. But what are your procedures for investigating a "Q" access candidate who was born in a third country, has a citizenship in a second and is now in the United States working on defense and nuclear propulsion matters—and has stated his intention to become a U.S. citizen?

Answer. Where the FBI has a representative covering an area overseas, a request will be made of that office for logical inquiries such as education, employment, criminal and security checks. Since FBI representatives abroad are not operational, these inquiries would be requested through the cooperative services of police and security agencies in the foreign country. In other areas, or where our representative is unable to arrange for active investigation, the State Department will be requested to assist in the investigation by conducting the necessary inquiries. Checks will also normally be made of appropriate U.S. agencies which could have a record concerning the person's activities abroad, e.g., the Central Intelligence Agency.

Question 22. Did an FBI agent conduct the inquiry in Greece? Do you know who he talked to about Veliotis in connection with character references?

Answer. The matter was sent to our representative in Rome (who covers Greece) to handle and he requested the assistance of the Regional Security Office (RSO), U.S. Embassy, Athens, Greece in carrying out the investigation. The information reported by the FBI was obtained by the RSO and the full extent of the actual inquiry conducted is not know although the data provided indicates that inquiries were made in the neighborhood where Mr. Veliotis resided and at his father's marine engineering office where he worked until he departed Greece for Canada in 1953.

Question 23. Did the FBI agent go to any of the educational institutions which Veliotis had indicated he had attended to verify his attendance there?

Answer. The RSO advised that Mr. Veliotis' education at St. Paul's College, Athens, could not be confirmed because records were unavailable.

Question 24. Did the agent contact the Greek military to verify his reported service in the Greek Navy?

Answer. The RSO advised it was not feasible to verify the claimed service in the Greek Royal Navy; however, during the neighborhood inquiry in Greece it was determined he attended the Greek Royal Naval Academy from 1944 to 1947.

Question 25. A Department of Energy adjudication file on Veliotis has been turned over to the Subcommittee. But it does not include the FBI's report. The Energy Department feels it is precluded from giving FBI documents to us. However, there are references in the Energy Department file to certain aspects of the Bureau's work. One is a reference to the "FBI memo dtd 8-26-77,"which is followed by these works:"Subject received 45 day imprisonment in accordance with Decision #10 in Piraeus Court of Misdemeanor for issuance of uncovered money orders."Then the words, "Not listed,"are added. Is it possible for you to give us a copy of the August 26, 1977 memo? If not, can you answer the following questions about information contained in it?

Answer. The Department of Justice is pursuing an active criminal investigation involving Mr. Veliotis and has determined that no information from FBI of Department of Justice records can be released at this time.

Question 26. Did the memo have any documents or xerox copies attached of the court records, arrest records or any other pertinent information?

Answer. The only details provided were those as stated in the response to an earlier question. No copies of any records were provided.

Question 27. From reading the memorandum, how firm is the information contained in the memorandum? Obviously, the adjudicator at Energy thought it was firm enough to include in his adjudication notations. Is there anything there to suggest the investigator who wrote the memo might have been confused or unsure of himself or his facts?

Answer. The description of the information is simply set forth in narrative form and there is nothing to suggest any confusion in reporting by the RSO.

Question 28. The Atomic Energy Commission personnel questionnaire Veliotis filled out indicates he had no previous arrest or conviction. Presumably, the FBI had access to that AEC questionnaire. Is the agent on the scene, or the official who wrote the memo of August 26, 1977, under any obligation to point out to Energy the contradictory information—that is, the arrest record and the fact that Veliotis was not acknowledging it in his AEC questionnaire?

Answer. The investigation was conducted abroad, but a copy of the AEC questionnaire was not forwarded overseas. The arrest and conviction information was reported by the FBI and the agency was in possession of the questionnaire. We did not highlight that this data was inconsistent with information provided on the AEC questionnaire when it was disseminated. Normally such discrepancies are specifically addressed.

Question 29. The AEC questionnaire indicates that Veliotis went to work in Canada in 1953 and that 1953 was the date of his emigration to Canada. Was that inconsistency noted in the FBI memo—that is, that he was in Canada from 1953 forward, yet he was convicted in Greece in 1954 of money order fraud?

Answer. The FBI reported the fact, place and date of the conviction buy we did not highlight the inconsistency this represented with his reported date of emigration to Canada.

Question 30. The Energy Department file on Veliotis also reveals that in 1973 Veliotis made a trip to the Soviet Union. All trips to Communist countries are to be reported to personnel security offices, according to the Industrial Security Manual. Is there any information in the FBI memorandum of August 26, 1977 to indicate that the FBI knew about the trip to Russia? Is there any indication that the Bureau looked into the question of whether or not Veliotis reported the trip?

Answer. The August 26, 1977 memorandum pertained only to inquiries made in Greece by the RSO. Based in part on the information provided concerning extensive travel abroad by Mr. Veliotis, a check was made of records of the Central Intelligence Agency. The Chief of Security at the Quincy Shipbuilding Division (where Mr. Veliotis was employed) was interviewed and advised he was aware of no derogatory information concerning Mr. Veliotis. There is no record of specific inquiry at Quincy Shipbuilding Division regarding the trip to the Soviet Union or whether or not it had been reported.

Question 31. Did the FBI obtain a copy of Veliotis' job application form at General Dynamics? If so, did it conflict in any ways with the information developed in Greece?

Answer. Mr. Veliotis' employment was verified through interviews at the Quincy Shipbuilding Division and there is no indication his application form was reviewed.

Question 32. Veliotis was a citizen of Greece and Canada before he became a cleared industrial security official in the United States. We know the FBI did some work on his background in Greece. Was any done in Canada? Was any effort made to check with RCMP on Veliotis? If not, why not? Should his name have been submitted to a kind of NAC in Canada?

Answer. An inquiry was also made in Canada. In response Canadian authorities provided a copy of the results of a prior inquiry conducted by them in 1973. This inquiry had been requested by the FBI on behalf of the Defense Investigative Services as part of an investigation they were conducting. No unfavorable information was developed concerning Mr. Veliotis while he was in Canada.

Question 33. Would the FBI accept as a certification of place and date of birth the document sent over in 1973 from the Mayor of Kranidion? Can the Bureau provide anything more substantive or reliable?

Answer. When other sources of confirmation are not available, applicants are requested to provide documentation for parts of their background. The fact that the material was provided by the applicant and not derived from an independent source would be clearly noted so that the information can be properly assessed.

In connection with Mr. Veliotis' birth, it is noted that in the August 26, 1977, memorandum information was reported from the RSO that the birth of Mr. Veliotis in Greece in 1926 was confirmed by records at Nauplia, Greece.

Question 34. Has the FBI any intention of recommending that a new and thorough personnel security inquiry be made on Veliotis to determine with some assurance what his past was?

Answer. When information becomes available indicating that additional investigation is need in order to clarify information previously reported to an agency, the FBI would contact that agency to arrange for whatever further inquiry would be considered necessary. In the present case, since Mr. Veliotis is no longer employed in a facility requiring access to classified information and no determination is needed at this time concerning that access, there does not appear to be sufficient basis for resuming the background inquiry at this point.

Senator NUNN. The hearing will adjourn until tomorrow morning at 9 o'clock.

[Whereupon, at 12:25 p.m., the subcommittee recessed to reconvene at 9 a.m., Wednesday, April 17, 1985.]

FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

WEDNESDAY, APRIL 17, 1985

U.S. Senate,
Permanent Subcommittee on Investigations,
Committee on Governmental Affairs,
Washington, DC.

The subcommittee met at 9:10 a.m., in room SD–342, Dirksen Senate Office Building, under authority of S. Res. 85, section 13, dated February 28, 1985, Hon. William V. Roth, Jr., chairman of the subcommittee, presiding.

Members of the subcommittee present: Senator William V. Roth, Jr., Republican, Delaware; Senator Sam Nunn, Democrat, Georgia; and Senator Albert Gore, Jr., Democrat, Tennessee.

Members of the professional staff present: Daniel F. Rinzel, chief counsel; Eleanore J. Hill, chief counsel to the minority; Katherine C. Bidden, chief clerk; John F. Sopko, assistant counsel to the minority; David Glendinning, staff counsel; Leonard A. Willis, Glenn W. Fry, and Fred Asselin, investigators for the minority; Sarah Presgrave, executive assistant to the chief counsel; Kathleen A. Dias, executive secretary to the chief counsel to the minority; and Mary Robertson, assistant chief clerk to the minority.

[Senators present at the convening of the hearing: Senators Roth and Nunn.]

Chairman Roth. The subcommittee will please be in order.

I would ask the Honorable Donald J. Devine of the Office of Personnel Management to please come forward. Just remain standing. Under the rules of the subcommittee, all witnesses are required to take the oath.

Do you swear the testimony you will give before this subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. Devine. I do.

Chairman Roth. Thank you. Please proceed, Mr. Devine.

TESTIMONY OF HON. DONALD J. DEVINE, OFFICE OF PERSONNEL MANAGEMENT

Mr. Devine. Thank you very much, Mr. Chairman and Senator Nunn. It's a great pleasure to be here today. I congratulate you on having this hearing. This is a very important subject, in my opinion, which has not received the appropriate level of attention for a long period of time. I especially appreciate working with your staff over the last 5 months as we have prepared for these hearings. It's been very welcome to us the legislative interest in a program which I truly believe before this administration, as the papers said today, truly was in shambles and has been ignored by and large for two decades.

Personnel investigations are a very important part of national security and an important part of staffing the Government with its best people. It's critical that the quality of background investigations and other investigations done by the Government be of the highest and still respect the rights to privacy of individuals.

Personnel investigations deal with two major issues. In fact, the inability to distinguish these two issues has been the major intellectual problem with the way we've dealt with personnel investigations. There are basically two areas:

Security, which is defined basically in terms of access to classified material and is under Executive Order 10450; and suitability, or general fitness for Federal employment, under Executive Order 10577, as it's been amended.

OPM has investigated both of these areas over the past 4 years and made major increases in the quality of both. We've had a tenfold increase in the number of our evaluations, and they have found several major problems. The first and foremost importance is the low-quality investigative product outside the Office of Personnel Management and the security agencies; second, a drying up of sources, especially from State and local governments, but also private firms, resulting from the Privacy Act restriction; third, inadequacy of adjudicative standards in many Government agencies; fourth, noncompliance with reinvestigation requirements in half of the Government; fifth, lack of uniform standards and position sensitivity designation and; sixth, habitual use of waivers for preappointment investigations without following proper procedure.

This has been a long history of problems, but in March 1983, after 20 years of essentially ignoring this problem, by both the legislative and the executive branches, President Reagan forcefully asserted the need for greater protection to our national security in the area of personnel security investigation, and established a broad-based review of personnel security under National Security Decision Directive 84 (NSDD-84).

Likewise, we at OPM had already begun starting in 1981 to deal with a major review of our programs and what we could do to upgrade them. The result, I think, has been success in improving the quality.

We standardized our investigative products and recommended a level of investigation appropriate to different levels of security and suitability needs.

It's important to have a quality appropriate to the level of need of the Government, but no higher. We must protect the rights of individuals, but we must also protect the right of Government to know.

There was a lot mentioned yesterday about the cost of the OPM product and, in fact, the cost of the OPM product is higher. But the fact is that the quality is higher, too. I think it's important that we pay for the right level of investigation, especially when we're talking about access to secret, top secret and compartmentalized information.

At OPM, we spent the last few years reviewing many studies—10 in all—and especially the Personnel Security Survey by the Director of the Central Intelligence Agency, on the essential elements necessary to a sound investigative product.

As a result of the comprehensive analysis, certain sources which were shown to be nonproductive were reduced or eliminated; periods of coverage were adjusted; and an appropriate balance among written, telephonic and personal inquires was developed. Subject interviews were added.

The result was a five-level investigative product—the national agency check with inquiries; minimum background investigation; limited background investigation; the full background investigation and the special background investigation—and together with our reinvestigative product, each appropriate to its appropriate level of security or suitability sensitivity.

The fact of the matter is that the OPM product uses twice the number of sources, for example, as the Defense Investigative Service based both on our own surveys, their own estimate and GAO's estimate. We don't think that there is any product that's better than ours or even equal to our outside of the security community.

Our most important customer is the Department of Energy and the Nation's important atomic energy secrets. The fact of the matter is, they prefer OPM because of the quality of the product that we give, especially since we've made these changes over the last few years.

The second thing we've done is we've recommended a model—a detailed model—to agencies to use in evaluating the sensitivity of positions, again, both from a security and a suitability standpoint. The goal of that sensitivity designation system is, again, neither to do too much investigating so that we are sensitive to individual rights, nor to do too little so that we can protect the national security.

Third, OPM is now adjudicating basic suitability and is requiring agencies to report back on investigations regarding what action they've taken on derogatory information. I'm ashamed to say that OPM did not do this before. It was changed late in the last administration and I'm glad to say we're back in that business again. We're probably going to get further into this area.

Fourth, OPM has significantly improved its training and instructional programs. We've had 85 briefing sessions in 1984 alone on the new interpretive guidance that we've issued through the Federal Personnel Manual system. We've had 100 security appraisals during the last 3½ years, and as I mentioned before, a tenfold expansion in OPM's oversight activity.

Fifth, OPM has set a concrete program for a long-term solution to a long-existing problem in the Government, and that is a surge and then decline of investigation cases which, in most cases, can't be anticipated because of change in law or change in contractors or turnover in personnel.

The fact of the matter is that our workload has shot up nearly 60 percent between 1983 and 1985 after a long period of relatively low levels of investigative activity. The main reason is that our major customer—Department of Energy—which reduced its background investigation requirements to 13,807 in 1982 increased it by 24 percent in 1983 and 42 percent in 1984 over the 1982 level. Much of this increase due to change in contractors at the Oak Ridge and Idaho Falls nuclear facilities and greatly increased protective services at the Savannah River site.

Likewise, USIA has given us increased workload for Radio Marti. The judicial agencies and the increasing number of investigations they've required also led to a large surge in workload.

We've done several things to try to meet that surge. First, we've increased the investigative work force by 40 percent over the last year and a half. Second, we've streamlined our reporting format. Third, we've accelerated development of automated scheduling and processing capability. Fourth, I have imposed mandatory overtime requirements. Fifth, I have tied awards to productivity increases. Sixth, I've reassigned administrative staff to the field. Seventh, I've developed a more cost-efficient investigative product. Eighth, most importantly in a major change in policy, we have been moving to a concept of a corps of permanent investigators consisting of OPM employees supplemented by an expanding contractor relationship with outside investigators, many of them previous OPM investigations. This measure is the only way we can meet the recurring surges and declines in work load without significant disruptions.

As a result of these actions, I expect to achieve the standard 60- to 65-day turnaround before the end of this calendar year and, more importantly, be able to meet future surges and decline in the workload.

Ninth, OPM has recommended a new emergency waiver check which we believe, if widely adopted, could remove a significant degree of the risks associated with appointments prior to investigation.

Tenth, a DOD select panel in 1982 recommended a new requirement for a strengthened periodic re-investigation which OPM has also adopted as its recommended re-investigative product. Again, if it were widely adopted, we would expect a much-improved product there, too.

And, finally, and most importantly, OPM has clarified the distinction between suitability and security. These are distinctions that are not always easy to make, but they're critical ones. They are the distinction between access to classified material and between simple ability to work for the Government, that is, fitness for employment.

The standards are different; the courts have required different standards for each. We believe that the suitabiity criteria should be used routinely for Federal employment and that security should be used sparingly and as a last resort, but that it should be used when it's appropriate.

The courts will recognize security decisions made if, in fact, they are truly security decisions and not hidden suitability ones or suitability ones taken under the cover of security ones.

It's been very apparent to me in our discussions with the other agencies of the Government and the NSDD-84 process, that agencies have difficulty recognizing the distinction between suitability and security. Much of the security community has made an opinion that they couldn't successfully survive in court with a security case. I don't think that's true.

The report that we made to the National Security Council, a preliminary report of the NSDD-84 process, makes that distinction and our installment 311 issued in January of this year makes that further clarification.

So we've made a lot of progress. What do we have to do for the future?

I think the first and most important thing is to continue the NSDD-84 process to its conclusion. It's made a major step forward in terms of making critical distinctions and suggesting that we should look at the revision of the Executive Order 10450 so that we have better guidelines.

Second, I believe now that OPM has established the guidelines more clearly, the time for more vigorous assertion of OPM's leadership role is at hand.

Over the past 4 years, OPM has worked through a large number of briefing and training sessions to clarify guidance long confused, to alert the agencies of the Government to the necessary changes that have to be made both to protect rights and to protect security.

We intend to give agencies time to upgrade their systems, but agencies not making progress will be reported.

I would like to end my statement, and I have much more which is in the formal statement which I ask you to put in the record. Again, I want to express my appreciation for these hearings. This has been an area in which OPM has been extremely interested over the past 4 years. I've looked forward to such a hearing for a long time to state some of the problems I see and, hopefully, have the executive and legislative branches involved in a constructive discussion regarding what we can do to solve these very serious problems and to upgrade our national security. Thank you, Mr. Chairman.

Chairman ROTH. Thank you, Mr. Devine. Your full statement will be included in the record.

I just have a few questions, and then I will defer to Senator Nunn. As you are well aware, there has been criticism of OPM for the greater expense and time required to complete its background investigations as compared with the Defense Investigative Service. In fact, the cost for an OPM case was $1,375 compared to only $500 for DIS, which conducted them three times as fast.

I wonder, how do you respond to those figures? Is there a valid reason for OPM's long form investigative reports compared to DIS's short form?

Mr. DEVINE. I think several things are important there. First, GAO's 1979 report—as I was concerned that they didn't mention yesterday—makes very clear that the DIS product does not include any overhead expense. That's one of the major cost differences. They don't charge retirement; they don't charge procurement expenses, leave, and other kinds of overhead expenses that I think are important to cost out front.

We believe that you should have the whole cost of the product out front so that our customers know what the service is. Obviously, for those that DIS will do services for outside of the Department of Defense, essentially what we have is a defense subsidy of other agencies, so they might think that that is a good deal for them.

However, I think it's also important to look at the quality. The GAO study in 1979 quoted findings that the average number of sources in a background investigation by the Defense Intelligence Service was 13, whereas OPM's number of sources was 32.8. We went back and asked DIS several years ago. They gave us similar figures, 13.4 and our figures at the time were 30.2.

We did another survey recently in which we found, again, 13.4 against 30 cases for ours.

So OPM's number of sources is double or more than the Defense Investigative Service's product. We have a better product, and I think one that is needed for top secret clearance that is granted in security cases for background investigation.

We think it's important that both personal sources—where the Defense Investigative Service does about 6, compared to 17 by OPM—and record sources—where DIS does about 7 against 13 by the OPM product—be done.

Our product is better than any of the other domestic products, with the single exception of the Secret Service one done by and for their own agents, and other than the security community like the Central Intelligence Agency.

I think it's important in this area to talk about quality and, of course, that's one of the reasons why the product takes longer. However, as I said in my testimony, we have much too long a period now. It was because of an unanticipated surge. We have a program which will end that backlog and get us back to the 60-day period we consider normal by the end of this year.

So, yes, ours is too long now. The difference is we have a program already underway which will not only solve this backlog problem, but will stop future ones from taking place when we get other surges and declines in the number of investigations.

Chairman ROTH. Now, it's my understanding that OPM does not have a say in determining which persons in an agency should be granted access to classified materials; OPM is merely responsible for conducting the background investigations; is that a fair statement?

Mr. DEVINE. Yes, sir; in terms of access to classified material, even under a separate Executive order, from either the security 10450 or the suitability 10577 OPM lacks authority. However, in terms of suggesting levels of suitability, appropriate levels of suitability, OPM does give a suggested guide on how that should be done, but not for access to classified material.

Chairman ROTH. In the case of top secret, reinvestigations are required every 5 years. As I understand it, no such requirement, however, is mandated for the hundreds of thousands of people who have a secret clearance. Therefore, I guess one could say it should have been no surprise to managers that William Holden Bell, who sold information to Polish intelligence, had a secret clearance that was 28 years old.

If it were to be mandated that all persons with secret, as well as top secret, clearances be reinvestigated fully, that is with more than a check of Federal arrest and conviction records, what would the cost be?

Mr. DEVINE. Our guidance under the Federal Personnel Manual system recommends that reinvestigations be done for secret clearance also, as well as top secret clearance; but since, again, access to classified information is not an OPM responsibility, all we can do is recommend it.

We do strongly recommend it and most agencies tend to follow it, at least on the nondefense side of the job.

Chairman ROTH. As you know, there has been some criticism, and it personally bothers me that little more than a Federal computer arrest and conviction check, and a check of reporting organizations is all it takes to get access to information which if improperly released could cause serious harm to the United States.

Some people suggested we slash the number of people with such clearances, and for those who require the clearances, conduct a full background investigation with personal interviews.

Do you see this as an appropriate solution? Again, do you have any idea what it would cost?

Mr. DEVINE. I believe that we probably do, although, as I mentioned, this isn't a direct area of our responsibility. But, obviously, since it is so closely related, I believe that we do have more clearances than we should and that we should look in and investigate and be sure that we are not overclssifying material and that we're not giving more clearances than we have to.

And, second, I do think that it would be useful to have more of a background check than NACI and certainly NAC. I don't think that a national agency check is sufficient for a background investigation for secret access.

We do not recommend a full background investigation, but what we call a limited background investigation for that area. It's much more cost efficient to do a limited background investigation that it is a full background investigation, and we think that would be appropriate.

It is well beyond a NACI, national agency check with inquiries, to say nothing of an agency check. We think that would be a major step ahead. It wouldn't cost much money, but I don't have any precise estimate of how much it would cost. I think whatever it would cost would be a good investment and that is why we recommend a limited background for secret—again, clearly not the NAC, which we can't recommend for anything, and not the NACI. We think we need a product at least at the level of the limited background and, of course, all of ours are minimum investigations. We say to the agency, if you think you need more than that, do it. I think at a minimum, we need the limited background investigation for the secret clearance.

Chairman ROTH. Senator Nunn.

Senator NUNN. Thank you. Mr. Devine, could you give us a little bit better idea about how your agency and the others that you deal with determine which investigative cases go to you and which ones go to the other agencies? I have read about the system, I have been through it—but it seems to me it is just a hodge-podge system and has very little in terms of analytical approach to it.

[At this point in the hearing, Senator Gore entered the hearing room.]

Senator NUNN. Are all these investigative services running around out there competing to see who can give the best service for the lowest price? It seems to me there is an element of that in it. It is awfully hard to compete if some pass on overhead and some do not. You make a valid observation, I think, that if Defense doesn't put any overhead in there, and you do, then it looks like to me somebody over at the Office of Management and Budget ought to be knocking heads.

I thought we had a Government who had somebody at the top of it that looked at this. If Defense is over there not passing on any overhead at all and you are over there having to charge twice as much for investigations and getting, as you would allege a bad rap for it, it seems to me something is wrong. We are supposed to be one Government.

[At this point in the hearing, Chairman Roth withdrew from the hearing room.]

Mr. DEVINE. We're not really competing. OPM, under Executive Order 10450, is to do all background investigations, except those that it delegated to other agencies. At the time of issuing Executive Order 10450, the Defense Investigative Service, Customs, IRS, Secret Service, State Department were doing their own investigations. OPM at that time delegated the authority to do investigations for their competitive service employees to those agencies. That delegation could be removed, and that certainly is one of the alternatives that may take place if we don't get proper cooperation on the level of quality that we think should exist.

It isn't competition; rather, it is a delegation to do work with an investigative force that already existed. But that doesn't mean that it has to stay that way, and it is something that I intend to look at.

Now the problem is, that's just for the competitive service. As far as contractors are concerned, we have no responsibility for them and, of course, for the uniformed military, we have no responsibility for them either. Our scope and reach has only been in the competitive service, although the Department of Energy has chosen us because of the quality of our product to do their contractor work, but they don't have to do that.

So I wouldn't really characterize it as competition, but rather delegation to certain agencies to do their own work, although there clearly is a problem of coordinating the whole picture, especially if you include the uniformed military and the contractors, which are outside of our scope completely.

Senator NUNN. On the overhead question, we heard testimony yesterday that the State Department had contracted out their investigative services at a cost of approximately $900 per personnel case. Certainly, the contractor in the private sector, if they have any business going at all, would have passed on overhead in their package. That would not seem to me to be explainable by your distinction between OPM and Defense.

Can you explain the difference between State Department costs and OPM costs; is that again, in your mind, a quality difference?

Mr. DEVINE. Unfortunately, I don't have the information on that, but I can say that we do have in our future plan to use private contractors. I'm certain that the State Department product does not do the national agency checks since we still do that for them, even if they contract it out. Clearly, that expense isn't included in the $800.

Senator **Nunn**. You mean you may be getting duplication on that function?

Mr. **Devine**. No; it wouldn't be duplication. They would know that we would do that for them so, therefore, they would only contract out the rest of the investigation.

Senator **Nunn**. I am informed State Department does their own national agency check. Does that mean we have two groups doing the same thing?

Mr. **Devine**. If they did, their own contractor wouldn't be charged for it either.

Senator **Nunn**. You said you did it and the State Departments says they do it. Are we getting two departments doing national Agency Checks on the same people?

Mr. **Devine**. We do it for the competitive service. I am interested to learn, if they are doing for the competitive service, then we do have something I'm not aware of. I appreciate you bringing it to my attention. I will check it out.

Senator **Nunn**. Could you check it out?

Mr. **Devine**. Yes, sir.

Senator **Nunn**. Would you look into the $900 price State Department is getting and try to give us an apples to apples comparison as to what they are doing compared to what you are doing?

Mr. **Devine**. Yes, sir; we will try to do that.

Senator **Nunn**. I don't mind friendly competition among agencies as long as we have an apples-to-apples way to compare it. It is mind boggling to sit here and hear different agencies doing the same security checks with no uniformity at all in what's required. We are one executive branch, although many parts. I just don't understand why somebody does not or has not gotten involved in trying to bring about some degree of consensus and uniformity. But I will get into that in a minute.

The other question is one of quality. I know that is a subjective judgment, and we are not going to solve it here in this hearing. The GAO yesterday testified they felt that the DIS product was more complete than the OPM product. You are saying yours has multiple sources. You say twice as many sources of checks as Defense, but the statement we heard yesterday from GAO was that your reports were open-ended and incomplete; that you left up to the agencies the further checking while the Defense service closed the loop, so to speak. If they found derogatory information, they pursued it.

It seems to me that is a quality, if that is correct, that tilts very much in favor of the Defense report, as opposed to OPM. If you don't pursue derogatory information, the number of sources seems to be secondary—you can certainly do a lot more sources if you don't pursue anything.

Mr. **Devine**. As I mentioned in my opening statement, March 6, 1980, OPM changed its procedure of moving to closure on national agency checks with inquiry investigations.

[At the point in the hearing, Chairman Roth entered the hearing room.]

Senator **Nunn**. You mean you do have closure now?

Mr. **Devine**. We moved into a situation in March 1980 where we moved from a case where we did closure to where we did not. In

1981, I began a review of that procedure. When we published our new guidance in basic installment 311 in January 1984, we began the formal change of that process where, again, as I mentioned, we do the basic suitability ourselves now before appointment, and once appointment is made, we categorize the issues and follow up with the agencies.

So I think the GAO criticism was appropriate for a period of time, and it's taken us a good deal of time to correct that mistake that was made in March 1960.

Senator NUNN. Wait; wait. That was another—you mean 1980, don't you?

Mr. DEVINE. 1980.

Senator NUNN. Let me ask this question then because my impression of GAO's testimony was that it was up to date. We will ask them to follow up on that, if they are here in the audience. If not, staff will pursue that.

I still don't hear you saying you have closure. It seems to me you are changing the definition of closure. Closure, defined by GAO, was the Defense Service itself closing the loop. What you are saying is now you send the information over to the agency and then you ask them how they closed the loop later on. That seems to me to be two different things all together. Are you saying that now you close the loop in your own investigation, or are you saying that you send it over to the agency and say, "Flay this information and you close the loop and let us know what you did?"

Mr. DEVINE. They are talking about the confrontational exit interview they do as their closure, which we are not allowed to do. It is part of the agencies adjudicative process.

Senator NUNN. Not allowed to do; I thought you said that was the mistake in 1980.

Mr. DEVINE. The mistake in 1980 was not closing the case, rather than having an interview with them. The problem is, we sent undeveloped material to the agency rather than categorizing what the material was. Remember, the suitability decision is essentially done by the agencies in the security area and by delegation from us in the suitability area, but we've taken back that delegation in the suitability area for what we call basic suitability, which is for applicants; we do it ourselves.

Once they are appointed, we now categorize it in categories and then follow up on what the agencies do through the adjudication. Since the security adjudication is basically done by the agencies, it makes some sense to have the suitability adjudication done there once they are on board, but now we follow up on it. And, again, in terms of the quality, I think you have to also ask about GAO; GAO is getting what clearly is a subsidized product. To them it looks like a good deal and one of the few that DOD is doing it for and all the others I know of are in the legislative branch also.

It's kind of a cheap service for the legislative branch which doesn't pass along the overhead charges.

Senator NUNN. Have you complained about that to David Stockman in OMB?

Mr. DEVINE. No, I haven't.

Senator NUNN. How about have you complained to Secretary Weinberger?

Mr. DEVINE. No. What I have done on this whole matter is that we have this under study at the NSDD-84 process. We've brought these issues up in that context, and we expect that these issues will be resolved in that context.

Senator NUNN. That brings me to my next question. I understand that the interagency group under the NSDD-84, which is the National Security Decision Directive, I understand that group has sent an option paper to the National Security Council seeking direction in May 1984, and that no response has been received from the National Security Council; is that correct?

Mr. DEVINE. The report was made to SIGI, which is a component of the National Security Council. My understanding of the meeting was that the interim report that we made was approved, unless it was disapproved subsequently by the National Security Council.

Senator NUNN. I thought there was a series of options, that you asked a series of questions to the National Security Council. I didn't visualize that as a report. What I thought you had done was ask a series of options for further clarification.

Are you saying you actually made a report to the National Security Council and you now consider it approved because they haven't responded?

Mr. DEVINE. Well, the SIGI considered the options and came to a conclusion.

Senator NUNN. So the paper was a set of recommendations that you now deem to have been approved by the National Security Council?

Mr. DEVINE. Well, insofar as two decisions were made that are critical to me—there are a lot of other things involved there—first that there is a distinction between suitability and security and that they should be pursued separately, and my issuance of basic installment 311 expressing that clarification between the two fulfilled that end of our responsibility.

Senator NUNN. And you believe that has been approved by the National Security Council?

Mr. DEVINE. Yes, sir.

Senator NUNN. You do?

Mr. DEVINE. Yes, sir.

Senator NUNN. So you now have full authority in that regard?

Mr. DEVINE. Well, I have as much authority as I have under a guidance document.

Senator NUNN. What is the second one that you believe you have gotten full authority on?

Mr. DEVINE. The second is to proceed with further discussions with the Attorney General and the interagency task force he sets up to come to final conclusion as to what we should do in the area of security.

Senator NUNN. That is where you started, was it not?

Mr. DEVINE. No, sir. As I mentioned, it's perhaps difficult to understand once the distinction is clearly made between security and suitability, but we spent months and months trying to get distinctions made between what suitability was and what security was so that we would know precisely what the area that we needed to study was.

What we did was we focused on access to classified information as being the critical distinction and that we should look at least at the option of amending Executive Order 10450 to have a more up-to-date set of criteria under security.

Senator NUNN. This thing is perplexing to me. I am getting more and more concerned in this area rather than less and less because you interpret what has happened with the option paper as having gone to NSC; that they have implicitly approved certain areas for your certain pursuit and the Department of Defense. I have a letter here, dated January 16, 1985, which, Mr. Chairman, I ask unanimous consent that it be put in the record.

Chairman ROTH. Without objection.

Senator NUNN. I have the wrong date. This letter is dated February 7, 1985, from the Secretary of Defense, and also a letter of January 16, 1985, from Mr. Devine to the Secretary. I would like both be put in the record.

Chairman ROTH. Without objection.

[The letters referred to were marked "Exhibits No. 15 and No. 16" for reference purposes and follow:]

EXHIBIT 15

OFFICE OF PERSONN
WASHINGTON, D.C.

Office of the Director

January 16, 1985

The Honorable Caspar W. Weinberger
Secretary of Defense
The Pentagon
Washington, DC 20301

Dear Mr. Weinberger:

As you are aware, I have been concerned about the national security and suitability investigations programs of the Department of Defense since even before I met with you on July 1, 1981 to discuss such matters. Under Executive Order 10450, I am required to oversee the Federal civilian personnel security programs, and under Executive Order 10577 (as amended in E.O. 12107), I am required to oversee and directly administer the civil service suitability programs. As I mentioned in my letter of January 27, 1982 to Mr. Taft, this led OPM to begin evaluation of the DOD security program. The appraisal evaluation process has now reached a stage where I feel it is important to discuss directly with you some serious matters which concern me.

A Report of the Committee on Appropriations of the House of Representatives, dated October 20, 1983, also is relevant to my concerns. That Report contains the following language:

> "The Committee believes that immediate action is required by the Department of Defense to correct these longstanding and potentially damaging deficiencies in personnel and industrial security. The Committee is therefore directing that the Secretary of Defense come to an agreement with the Director of Central Intelligence and the Director of the Office of Personnel Management as to what constitutes an adequate cost effective background investigation for military, civilian and industrial employees obtaining the various levels of security clearance."

In response to that directive, I am sending a copy of this letter to the Director of the CIA.

In a more recent development, Congress in enacting the DOD Authorization Act of 1985 included a rider exempting the Department of Defense from compliance "...before July 1, 1985...with...Basic Installment 311 of the Federal Personnel Manual...concerning personnel suitability, personnel security, and personnel investigations..." DOD also has placed a moratorium on implementing Installment 311. Congress acted in response to concerns expressed by Congresswoman Patricia Schroeder. The Committee was misled by correspondence which was offered as if it were the Department of Defense's official position on Basic Installment 311. This correspondence, dated April 8, 1984 over the signature of General Stillwell, was issued without prior concurrence and coordination among various affected Department of Defense officials. In a meeting with Dr. Korb, Mr. Cooke, General Stillwell, and Mr. Calhoun of DOD an agreement was reached between OPM and DOD concerning the Department's implementation of Basic Installment 311. This agreement was satisfactory to Dr. Korb, Mr. Cooke, and Mr. Calhoun, and resolved most of the outstanding differences between OPM and DOD.

Unfortunately, in spite of this group's best efforts to set the record straight, General Stillwell's position was misconstrued as the Department's official position. Of course, this was in direct contravention of the Administration's position. In a letter to the Chairman of the Senate Armed Services Committee, Director Stockman concurred with me in noting that the "Administration strongly opposes...and urges deletion" of those sections of the Bill which have (since then) been partially enacted as Section 1304 of the 1985 Defense Authorization Act. We believe this rider represents "an unnecessary infringement on Presidential authority." That the President ultimately decided, in the overall context of the Act, to sign the bill should not be construed as a reversal of the Administration's strong opposition to and dissatisfaction with these provisions.

The basic issues raised by DOD regarded suitability, rather than security. Two specific points were raised by those urging exemption from OPM's government-wide suitability authority: "implementation" of Installment 311 on suitability should await the outcome of NSDD-84 deliberations over personnel security; and, Installment 311 suitability provisions would impose significant administrative and financial burdens on DOD.

The first objection is entirely without merit. Both the drafters of and the participants in the NSDD-84 and SIG(I) review processes--including the DOD representatives--have agreed that NSDD-84 is concerned only with standards and requirements for access to classified information, not suitability issues. NSDD-84 did not suspend OPM's continued responsibility for and authority over the much broader governmentwide civilian suitability program, nor did it authorize agencies to suspend compliance with existing OPM security requirements pending the outcome of NSDD-84. Installment 311 simply clarifies how OPM already interprets its suitability guidelines and simply recodifies already existing security criteria. There is no reasonable basis for concluding that recommendations resulting from NSDD-84 deliberations would affect government-wide suitability requirements, nor that Installment 311 would inhibit changes to the security program under the NSDD-84 process.

As to the second point, we recognize that there may well be some additional costs and burdens resulting from the clarifications now made manifest to DOD in Basic Installment 311. We find, however, that the cost estimates noted in General Stillwell's correspondence were based on erroneous assumptions and have been greatly overstated. We have discussed with Dr. Korb how these costs could be minimized with cooperation between OPM and DOD. I believe that the costs resulting from Basic Installment 311 are extremely modest in comparison with the benefits and importance of improvements in this area. In any event, OPM stands ready to issue the clarifying language agreed to in my meeting with Dr. Korb to resolve the outstanding concerns of DOD.

As noted, the House Report on the 1984 Defense Appropriation Bill concluded that "immediate action is required...to correct...these long standing and potentially damaging deficiencies in personnel and industrial security." Unfortunately, it appears to us that this may in fact be correct. Fortunately, Installment 311 provides standards and models against which DOD and other agencies can measure the effectiveness of their own programs and upgrade them, while allowing for broad flexibility and agency discretion consistent with budgetary constraints.

I have every expectation that the Department of Defense shall be able to comply fully with Basic Installment 311 as of July 1, 1985. If there are any outstanding issues, differences, or concerns that may still prove troublesome to the Department, and which may require additional clarification, please do not hesitate to let me know at the earliest opportunity. I especially would appreciate the opportunity to discuss the status of DOD's security program with you and the Director of Central Intelligence at your earliest convenience.

Sincerely,

Donald J. Devine
Director

CC: Honorable William J. Casey
Director
Central Intelligence Agency

Honorable Lawrence J. Korb
Assistance Secretary for
Manpower, Installations and Logistics
Department of Defense

EXHIBIT 16

THE SECRETARY OF DEFENSE
WASHINGTON, THE DISTRICT OF COLUMBIA

7 FEB 1985

Honorable Donald J. Devine
Director
Office of Personnel Management
Washington, D.C. 20415

Dear Dr. Devine:

I have examined your January 16, 1985 letter regarding national security and suitability investigative programs at the Department of Defense as they relate to Basic Installment 311, issued by you on January 6, 1984.

I appreciate your continuing interest with respect to these programs in the Department of Defense.

After extensive study and review of Basic Installment 311, Deputy Secretary of Defense Taft on May 7, 1984 established the Department of Defense position. Legal and other problems identified by our review, including the matter of excessive administrative costs, necessitate that DoD implementation be held in abeyance until the President has had the opportunity to take action on the recommendations of the NSDD-84 study group, which was appointed by him and chaired by the Department of Justice, "to study the federal personnel security program and recommend appropriate revisions in existing Executive Orders, regulations, and guidelines."

Options and recommendations regarding the study areas to be examined were developed by the NSDD-84 group and forwarded to the Special Assistant to the President for National Security Affairs on May 1, 1984, by way of the Interagency Group/Countermeasures and the Senior Interagency Group/Intelligence. One of the recommendations is to draft a new Executive Order concerning access to classified information and to modify EO 10450 to make personnel security requirements clearly distinguishable from the general suitability requirements regarding federal employment. I understand that on April 19, 1984, in a personal appearance before the Senior Interagency Group/Intelligence you, as well as the SIG-I, supported all of the NSDD-84 group's recommendations. We were subsequently advised in October 1984, that the National Security Council would later in the year review the options paper and no problems were anticipated.

, It has long been our position and that of several other executive branch departments and agencies that play a key role in national security matters that Executive Order 10450, cited in your January 16, 1985 letter, no longer serves its intended purpose and that a new order should be issued. A new order to supersede the national security provisions of EO 10450, of course, would impact both in the personnel security and personnel suitability areas.

I am aware that the Department's personnel security program, the largest in the Federal Government, has not yet reached optimum effectiveness. During the last four years, we have intensively scrutinized the program, and significant improvements have been put in place. Last August, I met with General Stilwell and his staff to review additional measures that are feasible. Presently under consideration are actions designed for further improvement that were derived from an analysis of the effectiveness of the DoD Industrial security program completed on December 10, 1984.

Nevertheless, we believe that any program change as wide reaching as envisioned in Basic Installment 311, which has implicit impact on our military and industrial security programs, required the fullest coordination with all involved Executive Branch agencies. Basic Installment 311 was issued without that necessary coordination. On the other hand, the NSDD-84 study was directed by the President to assure a deliberate carefully constructed, fully coordinated effort to develop an integrated assessment of all personnel security programs of the Federal Government.

Accordingly, we will continue to cooperate with your office, as an element of the NSDD-84 study group, to develop recommendations for the President to reshape and upgrade the federal personnel security program. With the full cooperation of all participating agencies, we are confident that we can recommend to the President measures that will improve national personnel security.

Sincerely,

Senator **Nunn**. The Department of Defense clearly does not interpret that as being conclusive in any way. It says here:

> Nevertheless, we believe any program change as wide-reaching as that envisioned in Basic Installment 311, which has implicit impact on our military and industrial security programs, requires the fullest cooperation of all Executive Branch agencies. Basic Installment 311 was issued without that necessary cooperation. We will continue to cooperate with your office as elements to develop recommendations to upgrade * * *.

They make it very clear they are not going forward with any of this at this stage. We also have been informed by Mary Lawton, who headed up that interagency group, that none of this is final.

Mr. **Devine**. I recognize that I have a different interpretation of what happened in the Department of Defense.

Senator **Nunn**. How about the lady who headed up the interagency report for the Justice Department; your interpretation is totally different from hers also.

Mr. **Devine**. Well, that may be so also.

Senator **Nunn**. It looks like we have a first-class mess on our hands, doesn't it?

Mr. **Devine**. That's why it's critical that we move ahead on the NSDD-84 process, and why I have been in contact with the Office of the Attorney General that we get moving on this, and he's in agreement that we should.

Senator **Nunn**. I want to just bring up briefly one other thing and then I will have a lot more questions for the record. I know we have a time press. I will yield back to my colleagues to ask questions.

There are a whole series of critical reports throughout Government that we have solicited and gotten comments on on Basic Installment 311. It seems to me nobody agrees on it. I won't read all those, but I would, Mr. Chairman, like to put them in the record.

[Basic Installment 311 and the reports referred to were marked "Exhibit No. 17" and may be found in the files of the subcommitee.]

Senator **Nunn**. Are you satisfied with Basic Installment 311?

Mr. **Devine**. Well, they must have written differently to you than to me. My staff tells me that you only received 2 complaints out of 19 replies that were sent out on that. But, yes, I am satisfied with Basic Installment 311. I think it sets out a sound scheme. It's a recommended scheme. Agencies can deviate. We can work with agencies to deal with individual problems that exist. Most of the concerns that I've herd referred to the security section, not the suitability section, and it's the suitability section that I feel is what we have clarified.

The security we have not changed; we have made recommendations which we have always maintained in OPM are the proper quality that should be pursued. We don't believe there's been any change, but a significant clarification of a very confused issue in which this Government for 20 years has mixed suitability and security together. OPM tried in the past to preserve these distinctions by having separate suitability and security chapters, but the fact is that everybody looked at the security end rather than the suitability end.

We believe clearly on the suitability end that we have clarified that, and that agencies should have no problem moving ahead. Now, on the security, that clearly must await the result of the NSDD-84 process.

Senator **Nunn**. Well, we will furnish you a copy of the agencies' comments and there are numerous dissents on this whole 311 issue. I have more than five critical comments just as a little summary here. I won't go through all of it now. There also is a fundamental disagreement whether 311, as you described it, separates suitability and security—the agencies say it makes it worse.

Mr. **Devine**. You have to remember that these agencies have been working under a system where security and suitability have been confused for 20 years. Obviously, it's going to be difficult for them to recognize that distinction. It took me about 3 years in dealing with my staff to try to get them to see the distinction.

It is a subtle but critical difference, and the courts give different levels of severity to the criteria they use for each. The suitability criteria for basic employment with the Government, they hold high standards that we have to meet in a connection between the job and standards of due process, and so forth.

The problem in the Government is that we've been processing security cases under suitability for so long, the Government can't even recognize the distinction anymore. And that's what I've tried to change over the past 4 years through the discussions we had before the NSDD-84 process through the interagency task force that we chaired with DOD, and since then through the NSDD-84. It's been a tremendous education process.

Senator **Nunn**. Well, at the rate we are going, it is going to take three or four terms before we can get to that distinction. I mean, if it took you 3 years to convince your own staff, and we are still long way from having any agency agreement at all. We have this whole product sitting in limbo at NSC and have not heard from them in a year. You interpret that as a go-ahead, and the Justice Department and people who head the task force say it is not and State Department disagrees—you may be absolutely right; I am not quarreling with you. If you are the only one who believes it, we are not getting very far.

Mr. **Devine**. You know, Senator, this has been my frustration for the last year. We've had an Attorney General nomination that has been held up for a year. How can we have really——

Senator **Nunn** [interposing]. I was wondering when Congress was going to be blamed. [Laughter.]

Mr. **Devine**. I'm not blaming Congress. To me, it's a fact. How are we going to get serious negotiations going between the Attorney General and the Director of OPM where the Attorney General had to wait 1 year—I'm not even Director of OPM at this moment. We have a problem if we can't staff the——

Senator **Nunn** [interposing]. You had an Attorney General by the name of Smith there for 4 years, and you have been there for, how long, 4 years?

Mr. **Devine**. Yes, sir.

Senator **Nunn**. Well, it seems to me you are talking about the last 3 months rather than the last 4 years.

Mr. DEVINE. No, sir; the last year, the date as you correctly said——

Senator NUNN [interposing]. What was Smith doing down there? He didn't leave until late fall.

Mr. DEVINE. Yes, sir, but the fact is——

Senator NUNN [interposing]. Was he ineffective while he was there the last year or so?

Mr. DEVINE. Of course, he was not.

Senator NUNN. What is the point then?

Mr. DEVINE. It was my decision that it wouldn't make sense to get into this part of serious and far-reaching issue with an Attorney General who had already said he was leaving, and an already nominated new Attorney General coming in. I was waiting to begin discussions with the new Attorney General.

It seems to me that is only prudent. We have to start all over again with a new Attorney General and the only delay has been from April 1984 until today. And as I say, I have already talked with his office about it. He's very interested in moving ahead on this whole matter and, of course, he sits on the National Security Council, too, so that is very helpful.

So we had a hiatus during which it just didn't make sense to move too far ahead. And that's a decision I made. I can be criticized for it, but I think it's prudent that you wouldn't go into changes of this magnitude which have existed so long with so little attention from anyone that you could do that with a lameduck Attorney General and not do it with a new one who had already been nominated. I had every expectation after a couple of months it looked like it was going to be soon.

So, again, if there is criticism, I will gladly accept it, but it didn't seem to me to make sense to begin consultations on such a wide-ranging and serious subject when we hopefully had a new Attorney General coming on board shortly. It is no reflection on Mr. Smith, except he already announced he was going to leave.

Senator NUNN. I am not trying to assess blame. I am certainly not trying to lay it all at your feet on this question. It seems to me there is no coordination in this area at all. It is just a hodge-podge of everybody going in every different direction.

It seems to me somebody over all the agencies, like OMB, or someone speaking for the President has to get into this business. I guess that is where the National Security Council comes in. They, obviously, have not been acting on the option paper and that has been sitting there for a year. Either they are not interested in it or not a high item of priority, or they just have been inattentive.

I have some other questions, but I will submit them for the record, Mr. Chairman.

Chairman ROTH. Senator Gore.

Senator GORE. Thank you, Mr. Chairman. I would like to follow up briefly on the questions that the Senator from Georgia was pursuing. I don't quite understand this NSDD-84 process. I thought I did before your answers to Senator Nunn. My impression was that this was an options paper that was presented to the National Security Council and that it has been waiting at the National Security Council since May of last year for action.

You seem to indicate that you think the National Security Council has signed off on that; is that what you are saying?

Mr. **Devine**. There was a meeting of SIGI in which decisions were made on the options that were presented in that paper. The statement was made at the meeting that we should presume that they are approved unless we were told that the National Security Council wanted to review it. It is a subcomponent of the National Security Council.

Senator **Gore**. Now wait a minute. The interagency group was formed to study these issues. It was chaired by the Department of Justice; correct?

Mr. **Devine**. Yes, sir.

Senator **Gore**. All right, it was composed of Treasury, State, Defense, Justice, the FBI, CIA and you, OPM. This group drafted the options paper and submitted it to the National Security Council; correct? Am I right so far?

Mr. **Devine**. Committee on the National Security Council called SIGI.

Senator **Gore**. It was submitted to the National Security Council; right?

Mr. **Devine**. Yes.

Senator **Gore**. If they want to deal with it through a committee, but it was submitted to the National Security Council; right? OK. According to the chairman of the interagency group, there has been no response from the National Security Council to the options paper that was submitted to it for decision.

Now, you dispute the characterization of the chairman of that study group; is that correct?

Mr. **Devine**. No, sir; I think there is a consistency. We still might have a difference of opinion. I don't know what her opinion is on this, but one could say they haven't heard back from the National Security Council because SIGI disposed of it for them. So we wouldn't have heard back from the full National Security Council because the group under the National Security Council approved it.

Senator **Gore**. Well, why would Justice Department still be waiting for a response? Do you have special access to decisions of the SIGI? Does the SIGI speak for the NSC? Does the committee of the NSC speak for the NSC?

Mr. **Devine**. Obviously, the NSC makes or can make the final decision, but it can delegate it to the SIGI, too.

Senator **Gore**. Did the SIGI send you a written notification that it had signed off on this?

Mr. **Devine**. No, sir; I was at the meeting, and I recounted to you the discussion that took place as I was there.

Senator **Gore**. Was the chairman of the task force or the working group also there?

Mr. **Devine**. Yes, sir.

Senator **Gore**. Well, why would the chairman of the working group say no decision has been made?

Mr. **Devine**. She may have said that; I don't know precisely what she said. The statement you mentioned about not having hadn't heard back from the National Security Council could be true and still a decision could have been made by SIGI.

Senator GORE. Why is the Department of Defense still waiting for a decision of the NSC on this? They don't think the SIGI has decided this matter, do they?

Mr. DEVINE. I have no idea what they believe may or may not be the case.

Senator GORE. Well, when was this——

Mr. DEVINE [interposing]. Let me——

Senator GORE [interposing]. Go ahead.

Mr. DEVINE. Ms. Lawton was given the chairmanship of this committee by the Attorney General. The NSDD-84 Directive, however, mentions the Attorney General and myself. We are the responsible officials. I was waiting, as I said to Senator Nunn, for there to be a new Attorney General before I proceeded with the resolution of this.

I was aware that some had an interpretation that they thought that they needed some further response from the National Security Council. That was not my interpretation. I was awaiting the new Attorney General so that we could resolve that issue.

Again, it's one of the reasons, it seemed to me, it wouldn't make much sense to have the outgoing Attorney General make these critical decisions and, as Senator Nunn said, we need somebody who is in charge of this process governmentwide. And it is the Attorney General, in consultation with me, that's been given that authority by the President.

Senator GORE. All right now, you say the Attorney General in consultation with you. Isn't it a fact that before you make changes of the kind that you unilaterally made, you are required by law to consult with the other officials who share responsibility in this area, including the Attorney General?

Mr. DEVINE. As I say, the decision to make the distinction between suitability and security was made, and all I did through issuing basic installment 311 was to clarify the distinction between suitability and security.

Senator GORE. Didn't you change the sections that govern security?

Mr. DEVINE. They were put in as clarification.

Senator GORE. You changed the sections governing security clearances and you were——

Mr. DEVINE [interposing]. I clarified.

Senator GORE. And you are required by law, the Executive Order 10450, which governs your legal responsibilities in this area, you are required by law to consult with the Attorney General before making such changes, and you just chose to ignore the law and make an end run without consulting with them at all; isn't that a fact?

Mr. DEVINE. No, that's not true at all.

Senator GORE. Did you consult with them?

Mr. DEVINE. We have been consulting with the agencies since 1981——

Senator GORE [interposing]. I didn't ask that question, Mr. Devine. I asked whether or not you consulted the Attorney General, or Ms. Lawton, or the Attorney General's designee in this area before you issued changes to the national security clearance procedures that are embodied in basic installment 311. Did you consult with them?

Mr. **Devine**. I don't have to consult on guidance. The Administrative Procedures Act is very clear on guidance. You don't have to consult. That's our guidance. It's our product. The FPM installment 311 was supported by the administration in a letter to Congress. There are no legal impediments to what I did.

Senator **Gore**. Let me read you what the Secretary of Defense has to say about it:

> We believe that any program change as wide-reaching as envisioned in basic installment 311 which has implicit impact on our military and industrial security programs require the fullest coordination with all involved executive branch agencies. Basic installment 311 was issued without that necessary coordination.

Let me see if I understand you correctly. You have said two things here. You said just a moment ago you felt it was just a guidance so you were not required to consult, but a little while ago you said you didn't consult—correct me if I am wrong—you didn't consult because the Attorney General has said he was going to be leaving soon and you thought that it wouldn't be necessary to consult with someone who was going to be leaving soon.

Mr. **Devine**. Again, there are two parts of this problem—suitability and security. The issuance of FPM 311 was primarily in the suitability area and that, as I say, was agreed in the NSDD-84 process that that would not be a consideration of the NSDD-84 process, but would be left to OPM and there was no disagreement by any agency, including DOD or Department of Justice, on that issue.

Senator **Gore**. Well, there was no disagreement because you didn't ask anybody.

Mr. **Devine**. We certainly did. It was during the NSDD-84 process and it's in the paper that was signed off by SIGI.

Senator **Gore**. All these other people who were party to it are writing and complaining. The Department of Defense got a law exempting them from your unilateral action. Chapter 732, you say it just involves suitability. Chapter 732 is the chapter on security, is it not?

Mr. **Devine**. Yes, sir.

Senator **Gore**. And you changed that, did you not?

Mr. **Devine**. What we did is that we had to change 732 under security so that we could clarify suitability. That means that the wording was changed. But the fact is we did not change any of the security requirements, and we met with the Department of Defense, and they were concerned with some of the language that was in there. I wrote them and I told them that they shouldn't consider the security language binding. It's guidance, and that we would work out all of the security problems under the NSDD-84 process.

As far as I am concerned, the security parts of that are of no problem to anybody. That is our best interpretation of what the security portion of the existing guidelines are. We didn't make changes in that other than to clarify—as we very clearly said in there, if you read it—to clarify the distinction between security and suitability. And in the suitability area, we have full charge of that; everybody in the competitive service has their authority under suitability by delegation from us: and under the Administrative

Procedures Act, something that is done internally within an agency through its delegated procedures is handled as guidance through the FPM.

So on the security side, it's only if someone would interpret that 732 as a requirement for the agencies to meet now that they could have any concern with it. Now, I know DOD has concern with it. They have concern with it because they have some problems with the quality of their product, and they are afraid if they have to upgrade the quality of the product that it's going to cost a lot of money.

Senator **Gore**. No; they are concerned with what you did unilaterally, and they are not the only ones. The Treasury Department has also had to come and get a legal exemption from what you did. There was no consultation with them.

Mr. **Devine**. If they got a legal——

Senator **Gore** [interposing]. Let me finish.

Mr. **Devine**. If they got a legal exemption, it proves it is guidance and binding on them.

Senator **Gore**. These other agencies are complaining. Your unilateral action in the area over which you have responsibility has got the whole Government in an uproar about this security clearance procedure. Let me read you what the FCC——

Mr. **Devine** [interposing]. We should be in an uproar because the present system is bad, and we have to reform it. There is the only way we are going to get it done. That is why I am so glad we are having this hearing so this becomes a public question so we get it resolved.

Senator **Nunn**. I think we ought to stipulate we agree on that point. [Laughter.]

Senator **Gore**. That's right, but there are many others we disagree on. Let me read you what the FCC has to say about it. They note that under the new guidelines, which you unilaterally put out without consultation:

> A Federal employee who does not have access to secret material or facilities is subject to a more stringent background investigation than Federal employees who do have access to secret material or facilities.

Mr. **Devine**. Isn't that ridiculous?

Senator **Gore**. Yes.

Mr. **Devine**. We should change that, shouldn't we?

Senator **Gore**. That's what you did, Mr. Devine.

Mr. **Devine**. That's because I've said—I didn't change the security part of it. I only changed the suitability part of it, I'm not changing the security part of it because that has to be resolved through NSDD-84. That's precisely the point. Those are the old guidelines that, in fact, are not sufficient.

Senator **Gore**. Well, you are still taking unilateral action——

Mr. **Devine** [interposing]. You can't have it both ways.

Senator **Gore** [continuing]. Which gets us into that condition.

Mr. **Devine**. You can't have it both ways.

Senator **Gore**. Well, what do you mean by that?

Mr. **Devine**. You can't say that we both changed it and we didn't. That's what you're saying.

Senator **Gore**. No; I am saying you changed it without consultation with a way that leads to a ridiculous result, a result you characterized yourself as ridiculous.

Mr. **Devine**. Because of the fact we did not change the 732 to upgrade it where it should be upgraded.

Senator **Gore**. Because this executive order requires consultation; that was required in order to avoid inconsistent and ridiculous results of this kind. You chose on your own initiative to characterize your action in a way which you believe exempted you from the legal requirement to consult with the other agencies in this area. Now they are all writing and complaining; they are up here at the Congress asking for legal exemptions. It is really a mess. And the parts that were changed have created this timelag.

Seventeen of the twenty agencies that we asked about it had a consistent complaint about the amount of time that you are causing, that your agency is taking to respond to their questions. You acknowledge in your statement that there has been some inflation in the time. It has grown from 60 to a 75-day range to a 5-month range. And you state that one of the measures you have taken is to increase the number of investigators by 40 percent. In fact, what you are really doing is acknowledging the mistake you made when you took over by firing all those investigators in the first place; isn't that correct?

Mr. **Devine**. We only separated four or five investigators.

Senator **Gore**. Which represented——

Mr. **Devine** [interposing]. The fact of the matter is——

Senator **Gore** [interposing]. Which represented what percent?

Mr. **Devine**. One percent, roughly. The fact of the matter is, it takes too long to do them now. You are absolutely right; you get no argument from me. It was an unanticipated surge. The tradition in the area of doing investigations is that it had all to be done within the Government. I think that's foolish. I think that this kind of system cannot meet the surges and declines that you have in investigative workload.

I changed that so that we are not going to have that problem again, and the reason that the work force went down is that I also am under another act that says that I can't run negative balances in my revolving fund for this, and the fact of the matter is, that in September 1981, my staff informed me that if we continued where the caseload was going, we're going to have a $7.4 million negative balance in September 1981; $7.8 million by the end of fiscal 1981, and projected a further decline in cases that would give a deficit of $9 million by January 1982.

I had no recourse given the workload at that time, but to—not primarily fire—but not to hire more. I had to reduce that or I go into deficiency in the revolving fund, and that's precisely the roller coaster that this business has been on for the last 20 years.

And when there's surge, everything falls behind; when there is a decline, you fall into the red in the revolving fund account.

What I've done is set a rational management strategy that will forever deal with this up-and-down surge and decline in the workload in the Government. It is setting a solution to a problem that, unfortunately, now, yes, it's a terrible amount of time that we take, but we have a program that is going to get us current by the end of the year.

Senator GORE. In addition to the other problems which we focused on, there is at least one other, and that is the security investigations that you all are conducting do not appear to be very effective. As evidence of that, I want to cite you just one statistic.

During the period of time we surveyed from fiscal year 1980 to fiscal year 1984, there were security investigations on 138,252 people; 138,144 people were approved. Eight one-hundredths of 1 percent were turned down. That suggests to me either virtually all of the applicants are of a sterling character, and there is just a remarkable character profile among the people who apply, or that we have a system which is basically ineffective and incapable of weeding out people who should not have security clearance. Which do you believe it is?

Mr. DEVINE. Well, it's neither since we don't do the security adjudication, which is what results in whether action is taken or not. The security adjudication is done by the agencies.

In terms of our own work, in terms of the national agency checks with inquiries, that level of investigation obviously is not going to be turning down a very high percentage of individuals. The fact of the matter is, fortunately, most people are reasonably honest and NACI investigations should not be used for sensitive positions.

I am not sure where your statistics come from, whether they are NACI's or BI's, but in either case, if it's an NACI and we're doing the adjudications, one would suspect that at minimal level of investigation you are not going to find very much. If it's BI's, we don't do the adjudications.

Senator GORE. I understand you don't have jurisdiction over adjudication, but OPM runs compliance checks on agency adjudication programs, and they make decisions on the basis of the information that is provided them in the security checks. I guess your conclusion is that 99.92 percent of all the applicants are in fine shape——

Mr. DEVINE [interposing]. No, sir. As my testimony shows, we're very concerned about the quality of adjudication in the Government, and we've made some changes in the suitability area where we have authority over it. And I think it's critical that in the NSDD-84 process that we deal directly with this question of suitability and even the question as to whether it shouldn't be centralized in OPM.

Senator GORE. Well, I have other questions also which I will submit for the record because I know we have a time problem. I would like to conclude that this episode with the basic installment 311 is, in mind, really extraordinary, because this Executive order really requires consultation and where there is some question about whether consultation is necessary or not, it's obviously preferable to err on the side of consulting rather than create the kind of furor that is now raging throughout these agencies aimed at you and OPM because they feel that you have made an end run around the legal requirements and created a big mess.

Mr. DEVINE. Well, you are certainly entitled to your opinion, but I think the important thing is that the suitability area is clearly under our authority, and we can issue guidance in the suitability area without consultation with the agencies, although there was a great deal of informal consultation that went on, in any event, and also through the NSDD-84 process.

But if this has created some concern among the agencies, I say that's to the good. Let's solve these problems rather than hiding them under 20 years of neglect, and the fact of the matter is that this President started the NSDD-84 process and got us on the right track, and we're moving ahead and I'm very optimistic.

Senator GORE. We have been waiting for a year for a decision from NSC. Thank you, Mr. Chairman.

Chairman ROTH. Senator Nunn, I understand you have one more question.

Senator NUNN. Just one other question. Mr. Devine, you pretty clearly established jurisdiction in terms of suitability, as far as your interpretation of it. And I don't question that at this point. The question I have, who's in charge of overall security?

Mr. DEVINE. National Security Council in terms of security. If you are talking about in terms of changing the policy——

Senator NUNN [interposing]. Yes: I am.

Mr. DEVINE. The Attorney General and myself.

Senator NUNN. Clearly, the President has designated you two over the Department of Defense, over the Department of Energy, all of those? Do you have the authority to make those decisions?

Mr. DEVINE. Not decisions. We're going to recommend them to the National Security Council and the President.

Senator NUNN. So the National Security Council and the President is where we ought to be looking for this overview?

Mr. DEVINE. I think until the attorney General and I have——

Senator NUNN [interposing]. Who's been in charge for the last 4 years?

Mr. DEVINE. The Attorney General and myself.

Senator NUNN. Thank you.

Chairman ROTH. Thank you, Mr. Devine.

Mr. DEVINE. Thank you, Mr. Chairman.

Chairman ROTH. At this stage, we call forward Mr. Dalinsky. Senator Nunn, I am going to ask you if you would preside over the rest of the hearing.

Senator NUNN. Thank you, Mr. Chairman. I am going to have to be briefed by you over in the Intelligence Committee when I get over there. We will try to run these hearings as thoroughly and expeditiously as possible.

Without objection, we will put in the record the questionaire responses by the agencies which both myself and Senator Gore were referring to, and that will give everyone a chance to see where this matter stands, including Mr. Devine. The OPM, of course, can respond to those.

[At this point in the hearing, Chairman Roth withdrew from the hearing room.]

Senator NUNN [presiding]. We would like to keep the record open on that.

[Mr. Devine's prepared statement, with attachments, and responses to written questions follow:]

DONALD J. DEVINE

DIRECTOR DESIGNATE

U.S. OFFICE OF PERSONNEL MANAGEMENT'S

TESTIMONY ON PERSONNEL SECURITY

AND SUITABILITY

prepared for

THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

of the

COMMITTEE ON GOVERNMENTAL AFFAIRS

INTRODUCTION

I appreciate this opportunity to respond to the Senate Permanent Subcommittee's concerns regarding the Government-wide personnel security and suitability programs. Although responsibility for personnel security has been dispersed by law and executive order among various agencies, the Office of Personnel Management (OPM) is the only agency with government-wide policy-setting and oversight authority for personnel security among civilian employees. In addition, OPM has a broad jurisdictional basis and authority over the qualifications, fitness, and suitability of civil service applicants, appointees, and employees. Given this OPM role, it is appropriate for the Committee to request our views.

I. OPM'S ROLE IN PERSONNEL SECURITY AND SUITABILITY

1. A Brief Historical Overview

Some form of institutionalized selection and screening process has been in place, almost continuously, since President Grant's "Advisory Board of the Civil Service." With the assassination of President Garfield in 1883 by a federal job applicant, Congress codified the screening process by enactment of the Pendleton Act. Section 2 of this civil service Act provided for the promulgation of rules governing the "fitness" of applicants for the public service.

After passage of the Act and prior to World War I, investigations were primarily focused upon charges of misconduct, particularly violations of the political activity rule. Even in 1915, though, 72 investigations were recorded, including a dozen resulting from "unfitness" issues. It was not until 1917 that the Civil Service Commission ("Commission") initiated formal field investigations to determine "experience, fitness, character, success, and adaptability" of candidates for specific federal positions.

During World War I President Wilson issued a "confidential Executive Order" allowing heads of agencies to remove employees on grounds of "conduct, sympathies, or utterances, or because of other reasons growing out of the war" when retention of such employees would be "inimical to the public welfare."

After the War, the Commission greatly expanded its review of fitness and suitability. In 1920 it established a Division of Investigation and Review for certain Postmaster positions. In 1927 three thousand applicants for the Bureau of Prohibition were subject to background investigations. By 1938 the Investigations Division had a staff of almost 40 investigators, which number more than quadrupled during the next 2 years.

With the passage of the Hatch Act in 1939, Congress codified certain standards which had previously been promulgated in executive order and Commission regulations, and added a requirement to remove any employee with membership in any organization advocating the overthrow of the U.S. Government. Commencing in 1947 Congress granted summary removal authority to heads of such sensitive federal agencies as the State Department and CIA. In addition, Congress passed a number of laws, such as the Atomic Energy Act, the Institute of Inter-American Affairs Act, and the World Health Organization Act which contained special employee loyalty clearance requirements. After 1952 these personnel screening investigations were transferred from the FBI to the Civil Service Commission.

Public Law 733, enacted by the 81st Congress on August 26, 1950, established authority for a government-wide employee security program. The Act was made applicable to 11 named agencies, but later extended, under E.O. 10450, to all Government agencies. It provided agency heads with the authority to remove employees "when deemed necessary in the interest of national security." This Act represents the strongest indication of congressional intent that federal employment be consistent with, and conditioned on, security considerations.

President Eisenhower, expanding on the national security authority provided in the Act of 1950, issued Executive Order 10450 in 1953 to establish a government-wide employee security program, with the intent of protecting security interests without abusing constitutional rights. Philip Young, then Chairman of the Civil Service Commission, described the intent of the new Executive Order as it affected the government personnel selection system:

> "The basic objective....is to make sure that there is no employee on the federal payroll, nor any applicant appointed who can, because of his position, endanger the national security. The American people must be assured that federal employees are persons of integrity, high moral character, and unswerving loyalty to the U.S."

The next year, in 1954, the President issued Executive Order 10577 which set a separate investigative authority for suitability. This order promulgated revised civil service rules governing appointments into the civil service. Rule V authorized the Commission (now OPM) to "make appropriate investigations....of the qualifications and suitability of applicants for positions in the competitive service."

In 1966 Congress, through passage of Public Law 89-554, restated the President's nearly century-old statutory authority to establish a civil service employee screening and evaluation program and to prescribe rules of conduct for employees. Section 3301 of Title 5 of the U.S. Code specifically authorized the President to (1) prescribe rules for admission into the civil service (to "promote the efficiency of the service"); (2) ascertain fitness of applicants, and; (3) appoint individuals to make inquiries for such purpose. Section 7301 further provides authority for regulating employee conduct.

Part 731 (entitled "Suitability") of Title 5 of the Code of Federal Regulations, drawing upon the authorities stated above, authorizes OPM to deny appointment to applicants when necessary to "promote the efficiency of the service." It lists specific factors to be considered as a basis for disqualification, including misconduct in prior employment, excessive use of alcohol, abuse of narcotics, criminal or dishonest behavior, and other employment-related "issues."

In 1978 Congress again endorsed this screening authority by creating the U.S. Office of Personnel Management and transferring to it all of the Civil Service Commission's authority to implement employee suitability programs.

2. The Scope of OPM's Legal Authority

Personnel investigations deal with two major issues — personnel security and suitability. In distinguishing between security and suitability, it may be helpful to view security issues as primarily driven by "access" (to classified material) requirements. Although this distinction is somewhat artificial (national security may be affected by other than the compromise of classified information), it is the essential distinction. E.O. 10450 has, in fact, been viewed by the courts as bearing primarily on access-related issues, and the courts have generally equated "national security" with access to highly sensitive classified information. Suitability, by way of contrast, refers to the general fitness of an individual for a particular position and is based upon E.O. 10577. These distinctions and related standards become particularly germane during the adjudicative phase of the screening process.

Under executive order 10450 ("security requirements for government employment"), employees are to be "reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States." Furthermore, in order to assure "fair and equitable treatment", all persons employed are to be adjudged by "mutually consistent and no less than minimum standards and procedures."

E.O. 10450 places responsibility on the agency head for assuring that retention and employment is "clearly consistent with the interests of the national security." Appointment is to be made subject to investigation, the scope of which is determined by the degree of adverse effect the occupant of a particular position could bring about on the national security. Thus, the agency head has primary responsibility in designating a position as a sensitive one.

After an investigation on prospective appointees to sensitive positions is completed, the agency head is responsible for adjudicating the person's appropriateness for that position. Investigations of those employed in other than the competitive service are to be conducted by the agency if it has its own investigative capability. Otherwise, the agency may contract with OPM for investigative services.

Executive Order 10450 has long been recognized as a crucial element in the federal personnel screening program. Its principal value lies in the detailed and systematic scheme it prescribes for the conduct of such a program, including the distribution of responsibilities in national security matters.

Under Executive Order 10577 (as amended and now incorporated into 5 CFR) and various statues, OPM has an independent and unique responsibility and authority to make inquiry and determine fitness and suitability.

The Director of OPM is authorized and required to -

> "secure effective implementation of the civil service laws, rules, and regulations, and all Executive Orders imposing responsibilities on the Office by: (a) Investigating the qualifications and suitability of applicants for positions in the competitive service. The Director may require appointments to be made subject to investigations.... (b) Evaluating the effectiveness of (1) personnel policies, programs, and operations of

> Executive and other federal agencies subject to the jurisdiction of the office.. .(2) agency compliance with and enforcement of applicable laws, rules, regulations and office directives...."

In enforcing this provision of the Order, if the Director should determine that an employee is disqualified for federal employment, he may instruct an agency for a period of 1 year after appointment to separate or take other action against an employee serving an appointment subject to investigation. After the first year, OPM may require removal only on the basis of intentional false statement or deception, or fraud in examination or appointment. The Director may deny a disqualified person examination for and appointment to a competitive position, usually for a maximum 3-year period.

Prior to 1953 the Commission's investigations were based almost exclusively on its century-old suitability authority. Section 1753 of the Revised Statutes of the United States, dated March 3, 1871 (5 U.S.C. 631) provided the President with plenary powers for establishing civil service employment eligibility criteria. This authority was retained in the Pendleton Act of 1883 and is presently codified at 5 U.S.C. 3301. Sections 1301 and 1303 of Title 5 authorize OPM to "aid the President" in regulating the administration of the competitive service, including enforcement and oversight of agency implementation. A series of rules and executive orders were subsequently issued and codified in Title 5 of the United States Code (U.S.C.) and the Code of Federal Regulations (CFR). These statutes, executive orders, rules and regulations cumulatively provide a framework for a broad-based suitability program.

Commencing with World War I and continuing throughout the forties and early fifties, Congress and presidents added security and loyalty requirements to the Commission's underlying employee suitability program. These did not, however, affect the Commission's basic obligation to have a suitability screening program. After issuance of E.O. 10450, and particularly after President Johnson's expansion of national security criteria, efficiency and privacy concerns militated in favor of maximum investigative consistency between suitability and security-related investigative requirements. Both suitability and security have been concerns of the Commission and OPM ever since.

In addition to the broad authority noted above Congress has issued a number of more specific and detailed enactments requiring suitability and security determinations as a condition of federal employment or appointment. Title 5 provisions generally relate to merit principle practices, employee conduct, and proscriptions against certain types of activities, such as striking and alcohol abuse. The remaining provisions, scattered throughout Titles 22, 42, and 50 provide authorities and standards for other agencies in the conduct of their security programs. Such enactments include the following:

Title 5, U. S. Code: Sections 1103, 1104, 1304, 1305, 2301, 2302, 7301, 7311, 7312, 7352, 7531, 7532, 7533;

Title 22, U.S. Code: Sections 272(b), 2519, 2582;

Title 42, U.S. Code: Sections 1874, 2165, 2455;

Title 50, U.S. Code: Section 403;

OPM has government-wide responsibility in oversight and implementation of the various suitability, and civilian personnel security-related statutes and directives. All investigations of competitive service appointees other than those authorized under separate statute or delegated by agreement from OPM, are to be performed by OPM, and the investigative report is to be forwarded to the appointing agency. OPM can, and frequently does, conduct background investigations on other than competitive service personnel (eg. foreign service, excepted service, contractor employees, international civil service) but it does so merely as a service for other agencies, with no collateral authority or responsibilities of its own. OPM has no oversight, standard-setting, or policy-setting role outside the civilian workforce; and has no authority or jurisdiction over military and contractor personnel.

The most recent addition to OPM's list of responsibilities is in the area of computer security. Office of Management and Budget Circular No. A-71, Transmittal Memorandum No. 1, entitled "Security of Federal Automated Information Systems" requires the Office of Personnel Management to establish personnel security policies for Federal personnel associated with the design, operation or maintenance of Federal computer systems, or having access to data in Federal computer systems.

Under the various authorities by which the President and the Congress have delegated responsibilities to OPM for the effective administration of the competitive service, OPM has issued guidance and regulations pertaining to qualifications, knowledge, character, fitness, and suitability for appointment to a position in the competitive service. These can be found in parts and chapters 338, 731, 732, and 736 of Title 5 of the Code of Federal Regulations and of the Federal Personnel Manual.

The authority for security/suitability of individuals appointed to positions in the excepted service rests with the appointing agency head. The authority for security/suitability of individuals appointed to positions in the military service rests with the Department of Defense. The authority for security/suitability of contracter employees rests with the contracting agency head.

Despite the dispersal of responsibility and authority for employment suitability and personnel security among the various departments and agencies of the Executive branch, a certain degree of cooperation has developed between the excepted and competitive services. For example, OPM-promulgated employment standards for positions in the competitive service are frequently adopted by agency heads for their excepted service employees. Only in the uniformed and contractor "services" do significant variances exist from standards applied to the federal civilian workforce.

By law, security and adjudicative responsibilities over the civilian workforce are largely given to agency heads. Determining security-related position sensitivity is also discretionary with the agency head. The only real controls that OPM can effectively assert in the personnel security area is in its control over the investigative program consistent with the requirements of E.O. 10450, and its evaluations of agency civilian personnel security operations which under E.O. 10450 can eventuate in a report to the National Security Council.

3. Implementation of the Law

E.O. 10450 identifies broad categories of positions as sensitive and non-sensitive. The scope of investigation for each category is to be determined by the degree of adverse effect the occupant could have on the national security. The minimum investigation required (for non-sensitive positions) is a "national agency check with inquiries" to employers, schools references, and law enforcement agencies (NACI). All sensitive positions were to be subject to field "background investigations" (BIs). Other than requiring varying investigative coverages in relation to position sensitivity, the Order is somewhat ambiguous as to levels of sensitivity, and it provides only very general guidance as to the specific coverage of the Background Investigation.

The Order's sweeping definition of a sensitive position ("adverse effect on national security"), however, made it difficult for agencies to justify identical investigative inquiries for positions varying greatly in their potential impact on the national security. Therefore, on November 18, 1965, John W. Macy, Jr., then chairman of the Civil Service Commission, issued a letter (previously endorsed by President Johnson) requiring agencies to distinguish between two categories of sensitive positions: "critical-sensitive" and "non-critical sensitive." Under this new classification of position sensitivity, the NACI was extended as a baseline minimum requirement for "non-critical sensitive" positions -- although it was only set as a minimum, while only "critical-sensitive" positions required Background Investigation.

Although the effect of this letter was to sharply reduce the number of positions subject to background investigations, it failed to offer a mandatory investigative alternative for a wide range of sensitive positions now reduced in coverage to that of non-sensitive positions. The Commission was forced to modify its investigative product in conformance to agency needs. These modifications took the form of agreements with agencies to provide some variation of its standard Background Investigation. One product developed over time was the "Special Background Investigation" (SBI). Thus, when the intelligence community conditioned access to its documents on a 15-year period of coverage, the Commission expanded its inquiry from 5 to 15 years. Other unique products were developed. As a second example, when unusual qualifications had to be verified, the Commission modified its inquiry accordingly. If an agency required more information than that provided by an NACI, but less than a BI, then some limited form of investigation was conducted. Although both the CSC/OPM and the agencies have shown considerable resourcefulness in tailoring th[illegible] investigative products to fit position sensitivities, this approach was incremental, and did result in some inconsistent coverages because those products were not fully standardized.

As the government's leading investigative agency for the civilian workforce, OPM is responsible for the establishment of standards both in the security and suitability areas. As noted, this is done primarily through developing investigative standards. OPM takes several factors into consideration in developing such standards: distinctions between suitability and security; costs of investigations; and privacy and due process concerns as related to the level of risk associated with a position. A workable balance must be maintained between allowing for a variety of investigative coverages to accommodate a broad range of sensitivities, and the need to maintain a limited and discrete number of investigative products adequate to satisfy governmental interests without undue infringement on an individual's privacy.

Such a balance has been established and maintained through an inventory of five standard investigative products to meet a full range of suitability and security-related sensitivities: (1) a National Agency Check and Inquiries (NACI) investigation covering (through written inquiry) the person's activity for the most recent 5 years as the minimum investigation for Non-Sensitive positions; (2) an expanded NACI or Minimum Background Investigation (MBI) with a 5 year written and telephonic inquiry investigative period for lower risk positions at the Noncritical-Sensitive level and for "CONFIDENTIAL" access; (3) a Limited Background Investigation (LBI) involving personally-conducted interview coverage for the most recent 3 years, and written inquiry for 2 years beyond that for higher risk positions at the Noncritical-Sensitive level and for "SECRET" access; (4) a Background Investigation (BI) with personally-conducted interview coverage for the most recent 5 years (recommended expansion to 7 years) and written inquiries for the 2 years beyond that for positions at the Critical-Sensitive level and for "TOP SECRET" access; and (5) a 15 year Special Background Investigation (SBI) for persons entering Special-Sensitive positions or requiring access to Special Compartmented Information (SCI) under Director Central Intelligence Directive (DCID) 1/14. In addition, a Periodic Reinvestigation (PRI) is required every 5 years on each person occupying a position with "TOP SECRET" or SCI access.

The particular components of each investigative product have been carefully measured in terms of cost, utility, and productivity. The periods of coverage have been selected on the basis of survey data showing the amount of "significant adverse data" that would be lost for every year that is not covered. The selection of investigative procedures - written inquiry, personal interview, telephonic interview, or record search - was made on the basis of cost and anticipated productivity.

As an employer, the government shares similar concerns with that of most other employers; i.e., to retain responsible, honest, and law-abiding individuals, with good performance records and requisite qualifications. In determining the extent of coverage applicable to each level, the focus of agency concern would be on possible drug and alcohol abuse, criminal conduct, irresponsibility, and dishonesty. Well over 50 % of the total adverse data collected in these four categories result from police checks and interviews with former employers. Investigative coverage, therefore, for those levels in which "employer" interests predominate should emphasize these two sources in its investigative "mix." "Employer" interests, exclusive of "governmental" interests, predominate in non-sensitive or low-sensitivity positions.

Positions at the non-sensitive level have no "access" requirements, and offer little opportunity for fraud, abuse, or other injury to the national interest. A suitability determination would only include verification of prior employment, military status, education, a police check, and inquiries to listed references. If derogatory information is disclosed, then further investigation may be required. Otherwise, the NACI, together with any qualifying examinations and personal interviews ordinarily conducted by the agency, would suffice to protect such minimal interests as may be at risk.

Just a notch above the non-sensitive level are tens of thousands of positions which ordinarily require greater discretion and trustworthiness. Typically, the employer would want to have somewhat more detailed information about the applicant, particularly his prior employment record. The emphasis would be on "suitability" rather than "security," although, where access to "CONFIDENTIAL" data is required, some security consideration would be involved at the adjudication stage.

These low-sensitivity positions afford some, though limited, opportunity for fraud, abuse, and other injury to the national interest. Coverage is enhanced over the basic NACI, by inclusion of a credit check, telephone interviews with former employers, and mandatory follow-up on all unreturned inquiries. This "Minimum Background Investigation" while only marginally superior to that of the NACI, suffices to protect the government's slightly more sensitive interests, but are relatively non-obtrusive to maximize privacy protections.

Positions requiring more sensitive duties and functions than those noted above are of a distinctly different character. These have a direct or indirect bearing on the government's role as the custodian of national trust, security, and interest. Consequently, positions at these levels require not only the customary employee attributes of sound performance and responsibility, but also high standards of trust, confidentiality, reliability, and integrity.

Starting at the top, the most common purpose for a "Special Background Investigation" (SBI) is to gain access to "Special Compartmentalized Information" (SCI). The subject is to be entrusted with the nation's most sensitive secrets, particularly those related to intelligence operations. This highest sensitivity level is called "special sensitive." In almost all these instances intelligence agencies retain exclusive custody of such information, and those requiring access to it must conform to their clearance standards. The investigative coverage at this level conforms to the "DCID 1/14" requirements of the intelligence community.

Below the "special sensitive" level is the basic "critical sensitive" level. A position at this level, while providing for "TOP SECRET" access, may not require SCI access. In many cases no access may be necessary, but the level of fiduciary or policy-making responsibilities may offer considerable opportunities for waste, fraud, and other abuse. In order to maintain the public trust, incumbents of critical sensitive positions must meet stringent standards of integrity, confidentiality, and trust. Typically, top management officials, including most Schedule C and SES political appointees, would be covered under this level and would be subject to the "5-year BI."

And, finally, as a "bridge" between the relatively few top-level and highly sensitive positions and the large number of low or non-sensitive positions, OPM makes available its "Limited Background Investigation" (LBI) for the typical "noncritical-sensitive" position. At only a fraction of the cost of the BI, the still relatively nonobtrusive LBI focuses on the most relevant sources of information and most productive coverage. It will generally disclose enough information to provide the agency with a reliable profile of the applicant as a prospective candidate for positions of substantial public trust.

All investigations for the more sensitive positions involve a credit check, subject interview, and personal contacts with sources. OPM adds additional coverage at the request of the appointing agency for the appropriate level of sensitivity or to cover specific attributes that are particularly important to a risk assessment for employment in certain types of positions. A "standard" product, therefore, may have additional elements to deal with particular circumstances. Likewise, although OPM's standard BI product averages 30 personal and record sources, investigators are encouraged to resolve all issues regardless of the number of sources which must be developed.

Full field background investigations cover the full range of security and suitability issues. The primary emphasis in OPM is on quality; i.e., for the investigator to develop each case as completely as possible in a fair and objective manner. Questions asked range over a wide spectrum of employment-related matters such as drug/alcohol abuse, serious financial problems, criminal conduct, educational and professional qualifications, prior job performance, etc. Great care is taken to protect the privacy rights of the person investigated. OPM's investigators are under strong constraints with respect to what they can tell or ask a source about the subject. They cannot, for example, disclose any derogatory data they may have developed about the subject at any time. They must notify each source of the Privacy Act provision as provided in Part 736 of 5 C.F.R. These instructions and guidance cover OPM and agencies conducting investigations for employment/clearance in the competitive service under delegated authority from OPM. They also set the basic standards that generally govern investigations which OPM conducts on contractor personnel under requirements established by the Department of Energy under authority of the Atomic Energy Act of 1954.

OPM also provides guidance to agencies for designating position sensitivity. This designation is critical to the effectiveness of the Government's screening programs because the designation of position sensitivity determines the level of background investigation to be conducted. Once an agency has designated a position at a particular level of sensitivity, the agency is then responsible to assure that the applicant or incumbent has had a proper background check as a condition of employment or continued employment.

The initial point of contact between an applicant and OPM's investigative component may be as early as the submission of the employment application (SF 171) at OPM's examining office. If the application shows serious "issues" such as criminal conduct, court martial, or otherwise raises doubts on the applicant's suitability or qualifications, it is forwarded to OPM's Office of Personnel Investigations for a limited suitability investigation. After all the facts are in and the individual has been afforded the opportunity to comment, explain, object, etc., a decision is made as to whether the applicant meets basic eligibility criteria. This decision is appealable to the Merit Systems Protection Board.

If an individual applies directly with an agency, rather than through an OPM-sponsored competitive examination process, the agency is responsible for applying similar eligibility standards and "due process" procedures. After an individual is deemed eligible for a non-sensitive federal position, and is hired by an agency, the agency should submit (within 7 days) a request that OPM conduct an NACI on the appointee. For positions subject to background investigations, the agency should, under E.O. 10450, make no appointments until after the investigation is completed. However, because of urgent staffing or mission-accomplishment needs, the overwhelming majority of such positions are filled on the basis of an "emergency waiver", and investigation is commenced only after the individual is appointed.

In order to insure a maximum degree of adjudicative consistency and uniformity among agencies and fully implement its oversight role under E.O. 10450, OPM has instituted a procedure under which it notifies the agency of the "issues" disclosed in the investigative report and requires that agencies notify OPM of their decisions. Both the results of the NACI and the Background Investigation are forwarded to agencies who then have the primary adjudicative responsibility.

OPM has significantly improved its training and other instructional activities to give a greater measure of consistency and uniformity. New FPM chapters have been issued clarifying existing policies and procedures, and offering updated guidance and models to assist agencies in improving their internal operations. OPM officials have been holding workshops and arranging briefing sessions with personnel and security officers; 85 such briefing sessions and workshops have been held in 1984 alone. Special training courses have been developed.

Most importantly, in recent years OPM has expanded its oversight capability tenfold. Whereas OPM had only 1 or 2 staff members assigned to security appraisal work prior to 1981, we now have 10-12 individuals conducting this critical work. This staff of appraisal officers evaluates the effectiveness of agency personnel security and suitability programs. They cover a range of issues, relating to the quality of agency programs, such as the security of the systems themselves, timeliness, the quality of agency-conducted background investigations, the appropriateness of agency adjudications, and numerous other factors. The appraisal also includes an evaluation of the agency's computer security program and an assessment of the effectiveness of the agency's personnel suitability program. A report on deficiencies is prepared, and follow-up visits are scheduled for assistance and compliance. These appraisal visits provide an invaluable opportunity for hands-on training and problem-solving. During the last three and a half years, OPM has conducted over 90 such appraisals - almost three times more than had been conducted during the entire prior decade.

4. The Confusion Between Suitability and Security

One of the earlist findings of our increased appraisal activity was the general lack of understanding by agencies on the difference between suitability and security. It is important to understand these differences in the operation of coordinated suitability and security program, because distinctions between the two control the selection of standards, rights, and procedures to be applied.

Chapter 731 of the Federal Personnel Manual states that -

> "suitability means a requirement or requirements for Government employment having reference to a person's character, reputation, trustworthiness and fitness as related to the efficiency of the service."

Chapter 732 of the Federal Personnel Manual states that:

> "Security....is concerned with the employment and retention of persons in positions the duties of which relate to the protection and preservation of the military, economic, and production strength of the United States, including the security of the Government in domestic and foreign affairs, against or from espionage, sabotage, and subversions, and any and all other acts or situations likely to weaken or destroy the United States. Whenever a position requires regular use of or access to classified information, national security considerations are ordinarily present."

These distinctions between suitability (basic fitness for Federal employment) and security (fitness to hold a sensitive position, or have access to information that pertains to the national security) are not always easy to define, but they are both real and required by law.

Perhaps the main reason for confusion is the manner in which agencies delegate adjudicative responsibilities. Most agencies place the authority for making employment suitability decisions within the personnel office, while security decisions are made by the security office. This type of organizational alignment invites a lack of communication, inconsistent application of standards, and poor personnel management practices of diffused responsibility and accountability.

For these reasons, OPM encourages the centralization of adjudicative responsibility within an agency. If an agency has a predominately national security related mission, the security officer should be given responsibility for both suitability and security adjudication. On the other hand, the personnel office must assure that suitability remains a viable part of the program and does not lose its separate identity. Conversely, if an agency makes little or no use of classified information, and has a mission very unrelated to the national security, then a well-trained, mid - or senior-level personnel officer should be responsible for both suitability and security adjudication. Yet, even minor security requirements must be followed too. Other centralized arrangements are also possible -- as long as security and suitability remain two separate and identifiable programs.

In order to make the distinction between suitability and security easier for agencies, OPM has reissued FPM Chapter 731 with clarified guidance, and more clearly defined adjudicative procedures for suitability, and Chapter 732 with clarified security guidelines.

The new guidance makes more apparent the common "suitability" base that applies to all positions, and has shown that "security" standards (e.g. potential for compromise, contact with hostile agents, etc.) should be applied only after all "suitability" standards have been met. The guidance re-emphasizes that suitability, being the standard for all employment, must fully protect employee rights, and actions should be taken only when the interest of government efficiency so dictate. Agencies, therefore, are encouraged to use the suitability criteria routinely, and the more discretionary security authority sparingly and as a last resort -- but to use it when appropriate.

In short, OPM has clarified the distinction between suitability and security. The Government has taken two separate approaches to the very different issues of security and suitability. The President, under National Security Decision Directive 84 (NSDD-84) has initiated a comprehensive review of personnel security policy in the executive branch. That process has not as yet been completed. As regards suitability, guidance has been issued and training commenced to clarify agency responsibilities and to assure that decisions affecting employees are only taken to the degree to which they affect the "efficiency of the service."

5. Promoting The Efficiency Of The Service

In his 1981 inaugural, President Reagan promised to "make government work." Since that time it has been the goal of the Administration to utilize the federal workforce efficiently and effectively in all areas of personnel management. Shortly after taking office, the President established a President's Council on Integrity and Efficiency to end waste, fraud, and abuse in the government. This effort has already identified and set programs to eliminate $30 billion of wasteful, fraudulent, or abusive practices.

Not only does waste and fraud cost the taxpayer large sums of money, but, as the previous head of the anti-fraud campaign has noted, "public confidence is quickly eroded in a government that is poorly managed and easily defrauded." While the number of dishonest government workers is small, these few can do great damage. A recent GAO study estimated that almost one third of these losses is due to dishonest federal workers. A proper suitability program can limit these losses and promote the efficiency of the service through the selection of trustworthy employees.

A suitability program must assure that candidates have the experience and education claimed. The basic suitability program, therefore, must be concerned with the use of counterfeit credentials, the falsification of resumes, and the exaggeration of qualifications by individuals seeking employment. Fidelifacts, a New York based company that checks employee backgrounds, reports that it finds significant derogatory information in 30 percent of its job applicant cases. Such derogatory information generally involves stretching the truth, outright lying, or facts indicating the applicant is unqualified for the position. Similar results have been reported by other companies, such as the National Credential Verification Service (NCVS), which found that 7 out of every 20 applicant credentials had been falsified. According to an NCVS company official "the practice of falsification is rampant."

Not surprisingly, federal agencies have experienced similar results in conducting personnel suitability checks on civil service applicants. A sample survey of 5,200 investigative reports on applicants for critical-sensitive positions revealed a 25 percent rate of significant derogatory information, while 21 percent of applicant statements and forms had been falsified. Of the 1,730 "adverse factors" among the 5,204 cases surveyed in the DCI Personnel Security Survey, the subject admitted to the adverse data 47% of the time. The subject falsified data 361 times (21%) and was "not asked" about 385 times (23%). Although subjects tended to admit criminal records, they tended to falsify data concerning dishonesty, especially when the data was not a matter of record. The fact that the government has background investigations and paper inquiry checks minimizes these suitability problems.

As useful as detailed investigations are for the efficiency of the service, a proper suitability program must also be sensitive to the legitimate rights of its employees. Investigations must be related to the level of sensitivity of government positions and not be overly intrusive. Although courts have consistently upheld the government's right and interest in establishing loyalty, suitability, and security criteria for federal employment, they have stipulated that these criteria are to be selectively applied as a function of position sensitivity. Thus, a person may be deemed "unsuitable" on grounds of "security" for a position requiring access to classified information, or unsuitable to handle large sums of money, but perfectly well qualified and "suitable" for other positions in the federal service. In suitability cases, there must be at least a general relationship between the problem behavior found and the position to be filled (the so-called nexus between the behavior and the position held). Not only must this nexus be proven by the agency in the adjudicative process, and the applicant or employee be provided due process, but any decision is appealable to the Merit System Protection Board.

Effective screening programs with proper suitability due process protections, can aid in the good management of the government, as well as protect the national security. Many serious employment problems would have resulted but for timely disclosure through suitability investigations. The following are some recent examples of how an effective screening program can eliminate inefficient or even dangerous suitability practices within the Federal service.

(a) An "anesthesiologist" employed by an Army hospital had no valid medical degree or license to practice.

(b) A contractor employee working at the Kennedy Space Center was identified as an escaped convict serving life sentence for murder at a Georgia State prison.

(c) An applicant for a position as a Customs Inspector was a member of a cult plotting to use that position as point of entry for smuggling firearms into the U.S.

(d) An applicant for a position as prison guard failed to disclose relationship with a brother serving a life sentence at the same prison.

(e) An applicant for a computer programmer position at a nuclear weapons facility which had a capability for automated handling of "hot" nuclear materials was a member of a cult demanding total obedience to the cult leader and repudiation of U.S. laws.

(f) A routine background check disclosed that the wife of an important U.S. nuclear scientist was conducting a clandestine "affair" with a Soviet agent in a European country.

(g) A background check on a practical nurse at a Federal hospital revealed repeated prostitution and drug-related offenses over a 15 year period.

(h) An applicant for a position requiring extensive public contact showed a 30 year history of stealing, use and sale of narcotics, armed robbery, burglary, possession of heroin, assault with intent to kill.

(i) An applicant for a position in a Federal agency responsible for regulation and oversight of the banking industry had previously been prosecuted for bank fraud and embezzlement of over $500,000.

(j) A background investigation on a top management appointee disclosed 27 judgments totalling over $52,000; 32 tax liens totalling close to $400,000; several bankruptcies and foreclosures, numerous credit delinquencies.

Effective suitability and security programs of investigations promote the efficiency of the Federal civil service by screening out such inappropriate applicants.

II. PROBLEMS IN THE CURRENT SUITABILITY AND SECURITY PROGRAMS

OPM was asked to comment on specific problem areas previously identified by the Civil Service Commission, The General Accounting Office, various task forces, and Congressional hearings. Many of these problem areas are presently under review by the inter-agency task force established under NSDD-84. Upon completion of this review, many of these issues will be resolved. We will, however, address each of the issues specifically listed as requiring OPM comment.

I. Issuance of Clearances

According to a report dated October 18, 1983, prepared by GAO at the request of the Honorable Jack Brooks, Chairman of the Subcommittee on Legislation and National Security, there are well over four million Federal civilian, military and contractor employees with security clearances. Of a total of 5,137,280 Federal employees (civilian and military), more than half (51 percent) have some type of security clearance. GAO reported that some 2 percent (112,660) of Federal employees had "Sensitive Compartmented Information" (SCI) clearances; 9 percent (463,599) had TOP SECRET clearances; and 40 percent (2,054,906) had SECRET clearances. Most of the individuals with security clearances were civilian or military employees of the DoD or were contractor personnel working for DoD and cleared by the Defense Industrial Security Clearance Office (DISCO). Indeed, DoD accounts for approximately 85 percent of all clearances and 90 percent of SCI clearances.

Agency heads are responsible for designation of position sensitivity. If a position is critical-sensitive because it requires access to TOP SECRET information, the agency is the sole determinant of that requirement and sensitivity. OPM has not sought to monitor agency decisions, nor would it have authority to do so. That is not to say that we are unconcerned with the number of clearances in the Federal Government. For if too many positions are given SECRET access, for example, the number of sensitive positions necessarily increases. Not only are resources wasted if too many positions are classified sensitive, but pressures result to decrease the quality of investigative product for the positions which truly should be deemed sensitive. This does not appear to be a problem for non-DoD agencies, since the number of clearances issued and outstanding is relatively small. The need for access to classified information or restricted facilities is the exception rather than the rule. Most background checks are conducted because of fiduciary, policy-making, investigative or other sensitive, non access-related duties.

As regards DoD, we have no independent basis on which to question its need to issue this large a number of clearances. We are cognizant of a number of studies, conducted outside of OPM, which have been critical of both the criteria and procedures used by DoD to issue clearances. These studies have concluded that shortcomings in DoD's personnel security program may have resulted, in part, from budgetary constraints imposed by a high demand on the agency's investigative and adjudicative resources. We do know that the Defense Investigative Service absorbed a substantial Congressionally-mandated manpower reduction in 1976 which seriously eroded DoD's ability to do investigations. Yet, as a 1982 DoD Select Panel report noted, there is a relationship between the number of clearances granted and the quality of the investigative product.

2. Case Backlogs

Fluctuation in investigative workload has been a long-standing problem in government. Until recently, OPM provided a 60-75 day turnaround on a full field background investigation. Over the last two years, this turnaround has grown to 3, 4, and even 5 months. The growth in processing time has been the result of a large increase in demand by agencies for investigations. OPM has maintained an investigative workforce large enough to accommodate a predictable, fairly consistent level of work. Maintenance of an excess work capacity to accommodate "surges" would be wasteful.

As a government-wide "service" agency, most of OPM's investigative work is done on behalf of client agencies which may not be in a position to share estimates of their investigative requirements. Between 1980 and 1982, for example, OPM's workload dropped by over 20% to the lowest level it had experienced since 1973. Its inventory of cases dropped to a historical low of less than 3500. The revolving fund was running a deficit of one million dollars.

This situation dramatically reversed itself in 1983. Between 1983 and 1985, OPM's investigative workload shot up by 60%, and we estimate further 1985 increases by as much as 75% over 1982 to a level not experienced in almost 20 years. The Department of Energy which had reduced its BI requirements to 13,807 in 1982, increased it by 24% in 1983 and 42% in 1984 over the 1982 level. Much of this increase was due to changes of contractors at the Oak Ridge and Idaho Falls nuclear facilities, and greatly increased protective services at the Savannah River site. At the same time, the State Department, experiencing shortages of protective staff for its embassies abroad, redirected its investigative staff from background investigations and turned to OPM to do them. Likewise, USIA's "Radio Marti" initiative, FEMA's expanded involvement in emergency preparedness, and increased protective needs for the judicial agencies, all added hundreds of new cases to OPM's workload.

OPM responded to this situation by changing its management philosophy. First, I have increased our investigative workforce by 40 percent during the last year and a half. Second, I have streamlined our reporting format. Third, I have accelerated development of automated scheduling and processing capability. Fourth, I have imposed mandatory overtime requirements on investigators. Fifth, I have tied awards to productivity increases. Sixth, I have reassigned administrative staff to the field. Seventh, I have developed more cost-efficient investigative products. Eighth, in a major change in policy, I have commenced solicitation of proposals from private contracters to perform part of the investigations and transcription workload. This will allow us in the future to better respond to workload surges and declines, and prevent future backlogs. The overall result of these various steps will end the current situation. I expect to re-attain the standard 60-70 day turn-around by the end of this calendar year.

Most importantly, by permanently contracting out for transcription and other support services, by continually maintaining a core contracting out capacity for investigative services, and by full utilization of the ADP facilities which have begun to be phased in, OPM will be able in the future to respond rapidly to workload fluctuations.

We have, after a comprehensive review of all available surveys and reports, also eliminated costly and non-productive elements of the investigative process, such as mandatory personal interviews with character references or academicians and mandatory neighborhood checks in high density urban areas where a transient population is unlikely to disclose much useful information. We have also developed some optional products of reduced scope to preclude the need for unnecessary obtrusiveness. But these decisions were made entirely independent of timeliness or backlog concerns, and were based on the prudent balance of security interests, privacy and constitutional concerns, and related costs. The only change OPM has not been willing to make is in the quality of its investigative product.

3. Quality of Background Investigations

In May of 1980, The Director of Central Intelligence Security Committee published a Study entitled Investigative Scope and Adjudicative Procedures Among Intelligence Community Agencies. The purpose of the Study (better known by its abbreviated title - DCI Personnel Security Survey) was to evaluate the quality of investigations, especially the productivity of investigative sources and optional periods of coverage. Five member agencies provided the investigative file data used in the survey: the Defense Investigative Service, Office of Personnel Management, the Federal Bureau of Investigation, the Central Intelligence Agency, and the State Department. The data consisted of 5,204 background investigations, with adverse information disclosed in 1,261 of the cases, containing a cumulative total of 1, 730 separate "adverse factors" (i.e. items of derogatory information). The DCI Personnel Security Survey represents, to this day, the most comprehensive and ambitious effort ever undertaken to measure the effectiveness of investigative sources and coverage periods. As such, it is the best data presently available for basing decisions on the cost-effectiveness of sources, and for setting the most useful periods of coverage.

The DCI survey was used as the basic data to standardize the OPM investigative product from the several tailored products developed for agencies over the past two decades. To these data were added a total of 10 studies and surveys: two from DoD, five from OPM, one from the IRS, one from the GAO, and two conducted by inter-agency panels. As a result of a comprehensive analysis, certain sources which were shown to be non-productive were reduced or eliminated, periods of coverage were adjusted, and an appropriate balance among written, telephonic, and personal inquiries was developed. Subject interviews were added, based upon the experience of the Department of State, USIA, and DoD. The result was the five standard investigative products noted above -- the NACI, the MBI, the LBI, the BI, and the SBI -- and the periodic reinvestigation. We can now state, with a reasonable degree of confidence, that OPM's background investigations and its mix of investigative products (with the possible exception of those which use polygraphic interviews) are equal to or superior to that available from any other agency.

The minimum investigation conducted by OPM is that prescribed by Executive Order 10450 - the National Agency Check and Inquiries (NACI). Its coverage includes a check of the FBI's criminal history and security files, military records, and the files of other Federal investigative agencies, and written inquiries to former employers and supervisors, references, educational institutions, and State and local law enforcement agencies.

Use of the NACI varies substantially. While OPM uses the NACI as a minimum entrance investigation, other agencies use the NACI or even just the NAC portion as a basis for interim clearance or to bring someone on board in a critical-sensitive position before completion of the required BI. The NAC and the NACI have also been used for periodic reinvestigations for sensitive positions and have even served as a basis for SECRET clearances.

The NACI is recommended by OPM only for non-sensitive positions, since, at an approximate cost of $14 per case, it provides only modest protection against employment of criminal, irresponsible, unqualified, or incompetent employees. In 1965, an extensive survey of NACIs conducted by the Civil Service Commission disclosed that only 2% produced derogatory information. A 1969 Study showed that out of 400,000 NACIs, a total of 12,000 (3%) contained derogatory issues. Only 1,400 of those cases actually resulted in separation. A 1976 GAO survey of 96,000 NACIs disclosed 4% with significant derogatory information of which only 40 resulted in removal. More recent data developed by OPM shows results not appreciably different from prior surveys.

The "National Agency Check" (NAC) portion of the NACI provides limited, but important, information. The most productive part of the NAC is the FBI's criminal data file; yet even this contains only a small fraction (approx. 20%) of the criminal justice data available in State and local jurisdictions.

The "inquiries" portion of the NACI adds useful information to check the identify of the applicant, although employers and others often refuse to respond. Yet, the amount of information from the NACI is limited, so use of NACIs should be restricted only to its original purpose under E.O. 10450 - unquestionably non-sensitive positions of low grade and with little or no potential for injury to the national interest or the efficiency of the service.

Although the productivity of NACIs is relatively low, it would be unwise to reduce or eliminate NACIs altogether. On the contrary, NACIs must remain the major minimal investigative product for the large number of low-graded, non-sensitive positions. The NACI is unobtrusive and does identify some serious issues. We consider it inadequate for positions which require some substantial degree of discretionary or fiduciary responsibility, but appropriate for non-sensitive positions.

Recognizing the inadequacy of the NACI, OPM developed a low-cost investigative product that serves as an alternative to the NACI for positions that are of relatively low sensitivity but would, nevertheless, require a somewhat higher level of coverage. The newly introduced Minimum Background Investigation (MBI) attempts to correct the most serious shortcomings of the NACI. In addition to providing the same coverage as the NACI, it features a telephonic interview with the applicant's former employer, a credit check, and a follow-up with the various sources failing to respond to OPM's written inquiries. Although data are not yet available to determine how much more productive it is than the NACI, the low cost ($75.00) makes it a worthwhile investment.

The overwhelming majority of mid-level positions in the federal government do not fall into either the non-sensitive or critical-sensitive categories. They fall into the noncritical-sensitive categories for which no standardized investigative product has existed, even though past standards implicity recognized the need by declaring the NACI only the minimum quality product for this level of sensitivity. The introduction of the MBI at the lowest levels of sensitivity fills a major gap in coverage. However, as the sensitivity of functions moves up the scale approaching that of critical-sensitive (e.g. SECRET access, high but not top-level management), the MBI is not adequate to the task. The LBI (Limited Background Investigation) provides a basic, balanced, cost-effective investigative tool for more sensitive positions.

As a means of gauging the potential effectiveness of the LBI, it would be useful to compare it to that of the traditional BI. The 1980 DCI Personnel Security Survey demonstrated a remarkably high rate of productivity for the BI. Out of 5,204 cases reviewed, over 1,700 significant derogatory issues were disclosed, affecting almost every fourth applicant/appointee. 20% of these cases contained issues serious enough to warrant disqualification or separation - a total of 5% of all cases reviewed.

OPM's own surveys show somewhat higher rates of productivity and disqualification. A 1974 survey showed a total of 28% of the cases with derogatory issues, including 11% serious enough to warrant disqualification. A 1975 survey showed 35% with 9% serious enough to warrant disqualification. A 1977 survey of 1,000 cases showed 35% with 7% serious enough to warrant disqualification. A 1979 survey of 500 cases showed 28% with 6% serious enough to warrant disqualification. On average, therefore, OPM's experience with its own BIs indicates that 25-30% of all applicants/appointees for critical-sensitive positions have significant derogatory issues, with approximately 8% serious enough to warrant disqualification or removal. OPM's BI is 10 times more productive of issues than the NACI, and 30-40 times more productive of disqualifying issues.

The LBI bridges the two levels. The focus of the LBI's coverage is on the most recent 3 years, particularly the subject's most recent employment experience. Although the LBI includes the variety of sources found in the BI, the total number of contacts is markedly reduced. With the inclusion of a subject interview, we estimate that the LBI will provide enough information on which reasonable decisions can be made with a high rate of predictability and lower cost than the BI ($1,525 v. $650).

Since there is not a standard BI product outside OPM, the LBI may even successfully compete with other BIs. While OPM's BI normally averages 16 personal testimonies and 14 record testimonies per case, others average less than half that of OPM. Some also include no neighborhood coverage which a joint OPM/DoD study showed as being relatively productive outside of high-turnover urban areas. The neighborhood coverage in OPM's BI, in fact, produces close to 18% of adverse information developed during the investigation.

OPM, therefore, uses a broad mix of investigative products which are sensitive to the needs of government efficiency and security and which are sensitive to privacy concerns of individuals. Each product is of a quality only necessary to the legitimate needs of the government. But each has a quality sufficient to those needs.

4. Periodic Reinvestigations

In 1965 President Johnson endorsed a Civil Service Commission recommendation to provide a minimal update for critical-sensitive positions. Instructions to that effect are incorporated in Sec. 1-7 of FPM chapter 736. Under this, incumbents of special-sensitive or critical-sensitive positions are subject to periodic reinvestigation at 5-year intervals after placement. When circumstances warrant, agencies may, at their discretion, establish similar periodic reinvestigation requirements for incumbents of noncritical-sensitive positions.

As a regular feature of our personnel security appraisals, OPM reviews agency practice with regard to periodic reinvestigation of persons with TOP SECRET clearances. In one defense-related agency, we found that most components were not complying with periodic reinvestigation requirements even though department regulations included a provision to do so. In another non-defense agency, 17% of positions surveyed disclosed no evidence of reinvestigation. On the other hand, agencies with higher intelligence requirements, or very sensitive missions or very large financial impacts upon the economy tend to do periodic reinvestigations. Some critical agencies have set quotas to do only the most critical reinvestigations; while others do reinvestigation on their contractors but not their employees.

While there are important gaps, the results of our appraisals indicate general compliance by most agencies with the requirements for reinvestigation. These requirements are very minimal, however, and do not produce much information. The only requirement is for the subject to submit a new personnel security ouestionnaire, followed by a check of the official personnel file (OPF) and security file by the security officer. In 1982, the DoD Select Panel recommended that a "new requirement for a strengthened periodic reinvestigation be instituted" for SECRET, TOP SECRET, and SCI clearance. Among the elements to be included in the periodic reinvestigation (PRI) for TOP SECRET clearance were: subject interview by investigator; NAC, police, and credit checks; interviews with two employment and two developed references; a new PSQ; and a review of the OPF and security file.

OPM agreed with the Panel and the majority of the security community and, therefore, incorporated these elements into its recommended reinvestigation product. The DCI Security Survey found that these reinvestigations, even on individuals who had previously been subject to the "special background investigation", were productive of new and significant issues affecting an employee's continued eligibility for clearances. Frequently, an individual's opportunity for abuse or compromise of a position does not even materialize until after several years of government service. Financial or other circumstances may change radically over the years following the initial background investigation, but would never come to the attention of the employing agency without a periodic update. It is our hope that the NSDD-84 process will lead to the recommended PRI becoming the required reinvestigative product.

5. Emergency Appointment

E.O. 10450 has a general prohibition against pre-investigative appointments, but an exemption is available for emergency appointment "if the head of the departments or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records..."

A random sample of personnel security program reviews conducted by OPM under the authority of section 14 of Executive Order 10450, with regard to the use of "waivers", disclosed that about half the agencies issued waivers routinely or in a relatively high proportion of cases (22 to 35%) or had not properly documented the waivers given. For many, the "emergency" waiver provision has now become the ordinary and routine mode of appointment. In many cases, little or no justification is given and the authority to make the emergency exception is delegated far down the management chain of command.

The major difficulty with not performing investigations before employment is that an employment relationship may have existed for some period of time before action has to be taken. Employees often aggressively assert their "right" to continued employment in face of adverse agency action. Consequently, despite disclosure of significantly disqualifying information, agencies frequently choose to retain the appointee rather than risk litigation or controversy.

As an example, an extensive preemployment check was made by investigators in a subcomponent of an agency in which a high percentage of individuals were dropped from further consideration. On the basis of this preemployment screening, individuals were appointed to positions and then a background investigation was initiated with OPM. Despite the subsequent disclosure of derogatory issues, there was not a single instance of removal after appointment. By way of comparison, an intelligency agency conducted preappointment checks, which even included a polygraph examination, of its guard force followed by a background investigation. On the basis of information contained in the background investigation, an additional 10-12% of applicants were denied assignment.

The fact that it is much easier to deny employment, clearance, or access to an applicant than it is to remove from employment or revoke clearance is a reality in the national security process. Non-selection for appointment, or non-granting of a clearance, is not an appealable action as defined in Section 7512 of Title 5, United States Code. Removal, suspension, or other actions if taken against an on-board employee, however, are appealable. Greater procedural safeguards are accorded to employees than to applicants. Depriving an individual of that right, therefore, requires greater due process safeguards than if the individual were a mere applicant.

Agencies would experience severe hardships if every appointment were to be made on a post-investigative basis. The solution may well be the one which OPM has recommended in FPM chapter 732. Although we continue to endorse the post-investigative appointment as the proper and preferred mode whenever it can be accomplished without serious disruption of agency operations, we believe that some additional preliminary "checks" can be accomplished as part of the "emergency waiver" process. These pre-appointment checks could readily be accomplished in a period of 1-2 weeks and would offer opportunity for disclosure of as much as 35-40% of potentially derogatory issues, thereby safeguarding the government's interests without imposing undue hardships on the agency.

6. Legal Problems

An effective personnel security and suitability program must provide due process and privacy protections for its employees and sources of information. The whole relationship of investigative product quality to limitation of intrusiveness, and the due process protections written into the adjudicatory process are built around this principle. The Privacy Act, too, was intended to protect an individual's privacy against unwarranted government intrusion. Yet, in accomplishing this much-desired objective, the Act has seriously reduced the government's ability to collect information -- by an incredible 50 percent -- because of the unwillingness of sources to respond to inquiries. In comparing the quality of disqualifying adverse data (11% of all cases) developed just prior to enactment of the Privacy Act with the more recent findings, we have noted a steady and continuing decline over a 10-year period to the present level of 5%. A large number of employment sources refer to the Privacy Act as one of the major reasons for refusing to respond (in whole or in part) to questions concerning an applicant's employment history. Many of these companies are among the most important and largest employers in the country.

The Privacy Act requirement that the source be advised of the subject's right to see the investigative report, including the identity of the source, is the main reason for the problem. Most corporations do not want to expose themselves to possible legal suits from (former) employees regarding the information they give. While pledges of confidentiality may be offered, the law assumes that they will be used sparingly. If no independent verification can be obtained, information provided by a confidential source usually is not used as a disqualifying factor, regardless of the severity of the situation.

The most serious example of the difficulty of obtaining source material is from State and local governments, especially since they are one of the most useful and most productive sources of information available for personnel investigations. The DCI Personnel Security Survey disclosed that over 17% of all adverse issues involved criminal activity, and 26% involved drug and alcohol abuse, most of which activities are State or local offenses. Perhaps 25% of all adverse issues are derived from those sources. State and local police checks rank as the third most productive of actionable information (behind polygraphs and subject interviews). In comparing FBI data available through fingerprint checks with local law enforcement data, the latter proved to be 22 times more productive of unique derogatory information than the former.

A 1978 IRS Survey of 5,300 cases showed similar impressive results. Of the 1,063 derogatory issues contained in the cases, a total of 26% resulted from local police checks. A similar survey by OPM one year later showed productivity at 17-18%. In terms of periods of coverage, the police check exceeds all other sources (by a multiple of 8) for productivity beyond the 7th year.

It is obvious that State and local law enforcement checks are an essential and irreplaceable component of any background investigation. We are distressed, therefore, at the number of State and local law enforcement agencies that either do not provide OPM with information, or seriously restrict availability and access to that information since the enactment of the 1974 Privacy Act. Many State and local governments themselves have become increasingly sensitive to the issue of individual privacy and have interpreted their responsibilities in the area of individual privacy to include increased restrictions on the dissemination of criminal history data, even for the purpose of such law enforcement related activities as OPM's investigations. Other reasons cited by State and local law enforcement authorities for not providing access for personnel background investigations are: lack of sufficient money and staff to conduct these searches, refusal to recognize OPM's investigative program as law enforcement in nature, and OPM's lack of a National Crime Information Center (NCIC) number.

Many State and local governments will agree to furnish their record information only upon payment of a fee. OPM operates a nationwide investigative program and conducts hundreds of thousands of NACIs and more than 30,000 BIs annually. Because payment of fees would significantly increase the costs of our investigations, we have attempted to obtain appropriate law enforcement coverage through other means. However, the trend among State and local authorities for requiring payment of fees seems to be increasing, and we may need to reassess our position in the future in order to ensure that we are obtaining this crucially important information.

Our success in gaining access to local law enforcement data varies from jurisdiction to jurisdiction and year to year. Presently, for example, over 20% of all police departments will not respond to our written inquiries ("vouchers") routinely transmitted in the course of an NACI. These include such states as California, New York, Illinois, Delaware, Massachussets, and Minnessota, as well as large portions of Virginia, Florida, and Texas.

A number of jurisdictions are closed to our investigators even when they personally visit the local police department or record center. These include all of Massachussets, Delaware, Illinois State Headquarters, Washington State Headquarters, Oregon State Headquarters, parts of California, and Texas. While some jurisdictions will provide no data at all, still others will provide only conviction data but no arrest data.

And, finally, even after all local and State jurisdictions have been checked, gaps would still exist in instances where a crime may have been committed in a State other than that of residency or employment. OPM does not check police files in jurisdictions other than where the subject has resided or was employed. Access to the National Crime Information Center data bank would provide partial remedy to this problem.

Another difficult legal area for personnel investigation is the fact that investigators, although acting in good faith, are often personally sued for actions taken in the course of business. In Bivens vs. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971), the Supreme Court ruled that since the U.S. Government had not relinquished its sovereign immunity from suit, Federal employees such as investigators acting on behalf of the Government could be personally liable for a tort against constitutional rights.

A constitutional tort occurs when a Federal employee, acting within the scope of his official duties, violates a person's constitutional rights. Under present law, the injured person has no recourse against the U.S. Government. Suit can only be filed against the individual Federal employee, even though the latter may have been carrying out duties and responsibilities in accordance with the employing agency's rules and regulations.

Investigators are very much aware of the implications of the Bivens case, and the threat of lawsuit is a matter of continuing concern for them. They are not impressed with statistics and data showing that very few of these cases are successfully litigated. Most can not afford to have pending lawsuits interfering with opportunities for credit, home mortgages, etc. And even those who may feel totally confident of the outcome cannot feel comfortable with hundreds of thousands of dollars of prospective "damages" looming over them for a period of several years.

This heightened sense of anxiety has reduced the effectiveness and productivity of personnel investigators. From the investigator's viewpoint, it is "safer" to skirt issues which he knows to be "controversial" than to follow them up to conclusion and risk personal lawsuit. These very issues may be critical in an agency's ability to decide whether to entrust the applicant with some of the nation's most sensitive secrets.

Many Federal employees are responding to this problem by purchasing private insurance coverage. The Government does not pay the premiums on these policies which cost as much as $100 annually. I consider it to be a sad commentary on the government's role as an employer, when good, conscientious, honest employees are compelled to dig deep into their own pockets to protect themselves from the inherent and frequently unavoidable hazards of their jobs.

The Administration has long advocated an amendment of the Federal Tort Claims Act substituting the United States for the employee as the sole defendant. I have personally endorsed such an amendment on several occasions. I am convinced that the investigations program contains so many checks and controls against excessive or improper inquiries, that there is little chance of violation of any citizen's constitutional rights. And even if such violations were to occur, we have more than adequate administrative remedies with which to preclude future reoccurrence.

7. Adjudication and Due Process

No court has ever held that the Federal Government cannot inquire into the integrity, trustworthiness, loyalty or suitability of its employees; or that an individual's practice of First Amendment rights is beyond the pale of official inquiry. On the contrary, every judicial tribunal without exception has recognized and affirmed the Government's "compelling interest" in the loyalty and fitness of its employees, and its right to conduct inquiries and to take action to safeguard the national security.

Most court decisions have generally sought to maintain a practical and workable balance between the integrity of the Government and individual rights. In the past, concern has been expressed that the Supreme Court in Cole v. Young went too far against government security. In Cole v. Young, however, the highest court of the land acknowledged the constitutionality of Executive Order 10450 security procedures (and its antecedent Act of August 26, 1950). Not only did the Court endorse the broad discretionary powers accorded to agencies under E.O. 10450, but it affirmed the propriety of separate treatment of personnel security matters from those of employment suitability. Indeed, and perhaps more importantly, the court suggested at least one unambiguous test for the application of security standards and procedures, i.e., access to classified information.

Cole v. Young resulted from an agency's abuse of E.O. 10450 security procedures. Adverse personnel decisions had been rendered without adequate due process through the simple expedient of invoking "the national security." The Court felt constrained - in our opinion not without justification - to limit the application of the security adjudication provisions of E.O. 10450 only to sensitive positions such as those allowing access to classified materials.

In response to Cole v. Young, OPM's predecessor promulgated guidance to agencies restating the court's concern about excessive and unwarranted usage of security procedures and gave its own guidance to use suitability procedures "wherever possible." However, OPM has never proscribed the usage of national security procedures, and certainly does not do so now. It only requires that these procedures be used only when there is truly a national security question involved.

It is apparently true, nonetheless, that agencies have interpreted the "wherever possible" guidance to mean that national security procedures should never be utilized. Indeed, we have been told this orally. This is not an accurate interpretation of OPM's guidance. It is true that suitability procedures should be used in the normal state of affairs. Suitability is a consideration for every job. Protections to employees and applicants are greater under the suitability standard than they are under the security one. In terms of due process, it is appropriate to use suitability procedures as the norm since they give the benefit of the doubt to the employee. However, when grave matters of national security (e.g. TOP SECRET clearances) are involved, agencies should use the national security procedures.

Both the law and Executive Branch policy have long recognized the need for the integrity, trustworthiness and suitability of individuals in the Federal workforce and for the authority to refuse to appoint or to dismiss those who do not meet these standards. Congress, in Subchapter IV of Chapter 75 of Title 5 of the U.S. Code has specifically provided that an agency head has plenary authority for removal of employees "when he considers that action necessary in the interest of the national security." Under both law and Executive Order, the agency head's authority is clear. Whenever he considers it necessary to suspend or remove an employee in the interest of the national security, he is obligated to do so. He then must provide the employee with a written statement of charges, allow 30 days for response, offer the employee opportunity for a hearing, personally review the case, and submit a written statement of his decision. No appeal from the agency head's decision is provided.

Despite the apparent simplicity and fairness of this procedure, only recently -- for the first time in two decades -- has action been taken under this security authority. Apparently, this lack of use over time has been the result of the confusion between suitability and security procedures, and improper interpretation of the Civil Service Commission's "whenever possible" guidance. We appreciate the opportunity to re-clarify our intent: Section 5 U.S.C. 7532 and related E.O. 10450 procedures should be used when real issues of national security are involved. We also expect to raise this issue in the NSDD-84 process with the possibility of further clarification.

The standard for suitability removals as noted above, is that of the "efficiency of the service." In determining what effect a particular applicant or appointee would have on "the efficiency of the service," the threshold hinges on the "nexus" between an individual's performance or conduct and the service's efficiency. When derogatory information is obtained through an investigation and the adjudicator has determined that serious matters exist, an agency must provide due process. If the adjudication determines that employment is inappropriate, the decision is subject to review by the Merit Systems Protection Board (MSPB) in an adversarial proceeding in which the subject is entitled to representation by counsel, a trial-type hearing, and a further appeal to the United States Court of Appeals. An agency has the burden of proving that an applicant or appointee is not suitable for a particular position, and must demonstrate the seriousness of the past conduct, the contribution (or lack thereof) of social or environmental conditions, circumstances surrounding the disqualifying conduct, recency of the conduct, and other factors which may affect fitness.

The agency's burden becomes greater when an individual has been appointed prior to completion of the investigation, and has been performing the job. In this situation, the agency manager must satisfy more demanding "nexus" standards, is disadvantaged by the passage of time and satisfactory employment experience during a 6-9 month period, finds removal to be psychologically harder and more unpleasant, and, generally, views the removal process (as contrasted with the denial process) to be cumbersome and uncertain. So agencies often simply decide not to pursue these issues and retain employees who otherwise would have been deemed unsuitable.

Although nexus between a specific act and a specific position is normally required to sustain adjudicatory action, the MSPB has taken positive steps in recent cases to generalize certain behavior as having "a presumed nexus" because of the special heinousness of that behavior. Child molestation, drug pushing, and other serious criminal, dishonest or notoriously disgraceful conduct might be viewed under this doctrine as having a presumed nexus to all, or almost all, government employment situations. We are supportive of this line of interpretation which both protects individual rights but recognizes the need for a generalized "efficiency of the service" criterion.

We find the present legal enviornment generally supportive of an effective national security and suitability program. Some have been concerned about the Keyishian v. Board of Regents decision. Yet, here the Court held that before a state government could fire a State university professor -- tenured and entitled to academic freedom -- because of his subversive activities, the State first must prove not only that an individual is a member of an organization that advocates unlawful or violent goals, but also that the professor knew of that organization's goals and intended to further its unlawful aims. Thus, mere membership in the Communist Party or some other notoriously extremist group would not alone suffice to bar public academic employment. This Supreme Court decision, reached in the narrow context of a teaching position in a public university, clearly is different from the situation of occupants of sensitive positions in government. The Court has never taken the remarkable leap in logic feared even by some who are very sensitive to the needs of national security. Rather, courts have taken a reasonably balanced position between the interests of the individual and the government.

It is essential that agency adjudicative actions are fair, provide a standardized due process, and provide for employee protections. If so, they will pass judicial due-process review. Serious due process protections, appropriate to different levels of suitability and security, can both protect the individual and the government. OPM guidance and oversight acts within that context. OPM now characterizes and ranks issues in cases according to their seriousness, monitors agency actions on serious issues in individual adjudicative cases, and follows up with agencies thereafter. OPM has also clarified standards for adjudication which provides guidance and a point of reference for fair and consistent application throughout federal agencies.

8. Investigator Training

Effective and conscientious implementation of standards requires well-trained personnel. Section 2-8 of FPM chapter 736 states that training of personnel investigators should provide a thorough grounding in the fundamentals of personnel investigations and agency missions. It encourages periodic refresher training to update skills and assure continuing investigative competence. As a part of its appraisal and oversight responsibilities, OPM evaluates the scope and quality of training provided to investigators by agencies with delegated investigation authority, and makes findings and recommendations to improve or upgrade such training as necessary. Our most recent oversight review has revealed that:

o Defense Investigative Service investigators receive their training at the Defense Security Institute (DSI), Richmond, Virginia. Investigators average three to six weeks in the field before they report to the Institute. During their initial period in the field their supervisors must follow an on-the-job training guideline. Formal training at the Institute is four weeks with 25 to 30 students in each class. The formal training consists of a review of authorities, scope and coverage of the various investigations conducted by DIS, sources of information, interviewing techniques, and reporting. If an investigator has academic difficulties while attending the Institute, a report is sent to the individual's region for more follow-up before credentials are issued. DIS also conducts a one week field extension exercise for personnel in the regions who have not received formal training for five or more years.

o Customs Service. Personnel investigations are conducted by Series 1811 Criminal Investigators as a collateral duty. Investigators are issued an instruction manual and are trained by field supervisors who provide on-the-job training. A formal training package is being developed for use at the Custom Service Basic Agents Training School, and about 4 hours is expected to be reserved for personnel investigations instruction.

o United States Secret Service. Special agents attend an 8 week course with one day reserved for personnel investigations. Most of the special agent's training is based on work experience. Each investigation is coordinated by a journeyman level investigator, while subordinate agents work under his guidance. Personnel investigations are conducted as a collateral duty.

o Internal Revenue Service. IRS uses series 1810 general investigators, who attend a formal one week training course on conducting and reporting personnel investigations. IRS investigators spend approximately 75-80% of their time conducting personnel investigations. In addition to formal training, they receive 3-6 months of on-the-job training with senior investigators. Series 1811 criminal investigators at IRS generally spend only 10-15% of their time conducting personnel investigations after 3 days of formal training.

o Peace Corps. The agency has "contracted out" its personnel investigation needs. The Director of Security assigns cases, sets standards, and reviews each investigation for scope and coverage. He generally relies on OPM guidelines for the scope, coverage and conduct of personnel investigations.

o The Federal Bureau of Investigation uses special agents in a collateral duty capacity to conduct personnel investigations. Agents receive instruction in conducting and reporting background investigations as a part of their initial training at the FBI Academy.

The agency is currently in the process of developing a more extensive training course for personnel investigations. On-the-job training by senior agents remains the basic form of instruction.

o State Department. Investigations are conducted as a collateral duty by criminal investigators. Criminal investigators attend a 12-14 week training session at the Federal Law Enforcement Training Center in Glencoe, Georgia. Some of the subjects offered at the center (e.g. interrogation techniques) are useful in both criminal and personnel investigations. At the conclusion of the FLETC training, an additional 3-4 weeks of training is provided by the security staff at State Department Headquarters with "some" focus on personnel investigations. Journeyman agents are encouraged to enroll in department-sponsored courses, some of which deal with personnel investigations. The Department currently contracts with retired federal investigators or uses OPM directly to conduct most of its personnel investigations.

o Federal Law Enforcement Training Center. The center does not offer any personnel investigations training program, but agencies that use its facilities may teach the subject.

The Office of Personnel Management has an extensive on-the-job and formal training and retraining program for its personnel investigators. Investigations are conducted by series 1810 investigators as a primary duty. After a short orientation session, the initial training consists of 2-3 months of hands-on, job experience under the daily observation of a supervisor or senior investigator. This is followed by one week of intensive formal classroom training covering authorities, scope, coverage, sources, interviewing techniques, reporting, and adjudication. After an additional 2-3 months of closely supervised job training, the investigator is ready for independent work. Throughout his career the investigator is subject to continuing intensive review of all completed investigations. Supervisory or senior investigators conduct periodic reinterviews of selected sources and are required to accompany each investigator annually on field visits to evaluate techniques, practices, habits, etc. Formal expanded skills training is provided to investigators at the GS-9, 11, 12 and supervisory levels.

Refresher courses, seminars, and conferences are held on a regular basis to keep investigators and managers abreast of changes in the program. With the assistance of a contractor, we are presently developing a more comprehensive two week training program devoted entirely to conducting and reporting personnel investigations. This course will be offered to other federal agencies as a precedent for greater sharing and uniformity in personnel investigations.

Based on agency reaction and our experience with a prototype training program, we intend, as part of our FY-85 work plan, to commence development of a uniform program and standards in concert with other agencies. It would include expert instructors from the public and private sector. Special attention would be directed towards such sensitive matters as subject interviews, First Amendment rights, Privacy Act requirements, etc. A series of advanced and refresher courses would be offered for up-date and continuity. Successful completion of the courses would assure a base level of competency and uniformity in the investigative product, protection of civil liberties, fair adjudication, and appropriate action to protect service efficiency and the national interest.

I appreciate this opportunity to testify to the subcommittee regarding the status of the government's suitability and security investigation programs. Their proper administration is essential to the efficiency of government operations and the national security. The subcommittee is to be congratulated for its interest in these important matters and for conducting this oversight hearing.

I will be pleased to answer any questions.

Q. The Department of State has submitted a statement for this hearing wherein they claim that they stopped referring cases to OPM approximately one year ago because of OPM's heavy workload and timeliness problems. How many other departments or agencies have done so because of such problems?

We know of no other department or agency that has discontinued referrals to OPM because of timeliness problems. It is noteworthy, however, that the Department of State has been conducting its own investigations for several decades. In 1982/83 it was forced to reassign most of its investigators to embassy security duty abroad, and began experiencing severe timeliness problems similar to those of OPM. Subsequently, it referred over 1,500 cases to OPM, thereby adding to OPM's backlog, but relieving pressures on its own resources.

Q. To replace OPM's investigative function, the State Department has now contracted out its workload to retired federal investigators. State has told us that now they are able to complete their full field investigations in 60 days which is faster than OPM could do a National Agency Check. Additionally, the State Department says a full field investigation costs in the range of $900 for the same quality work that OPM does for $1,600. Should other civilian agencies contract out like the State Department to get the same quality work cheaper and faster than with OPM?

In recent months, OPM itself has moved towards a balanced mix of contractor and employee personnel. For the short term, in order to regain our 60-day turnaround time, we intend contracting with one or more private sector national concerns for completion of several thousand backlogged cases. For the longer term, we have been soliciting individual investigator contractors - including many retired Federal investigators - to supplement our regular staff of full-time employees whenever the workload significantly exceeds our capacity to handle it. This latter group will prove invaluable in removing the historical cyclical stresses and timeliness slippages resulting from widely fluctuating surges of work. We do not recommend, however, that either OPM or the Government in general should give up its core ability to conduct either suitability or national-security based investigations.

On the issue of comparative costs, we contacted the State Department for a more detailed breakdown. At that time we learned that State's $900 cost is merely an estimate. Mr. Clark M. Dittmer, Assistant Director for Personnel Security and Investigations stated that they do not have an accurate breakdown, and he was unwilling to commit the Department to a specific cost figure. However, we have identified several major differences between their cost and ours:

a) Although State's contractors (retired investigators) are responsible for absorbing the costs of office space, supplies, telephone, and similar overhead items as part of their final product, the agency gives the contractors extensive use of State's facilities.

b) The Department's background investigation generally contains 15 percent fewer sources than OPM's.

c) Since State's investigators are retired Federal employees, they do not charge back to the agency many of the ordinary expenses of employment. For example, since they are already receiving retirement benefits and are enrolled in annuitant health plans, there is no additional cost to the agency for these benefits. Also, State's contract investigators do not have to make adjustments for annual or sick leave usage, or charge overtime rates for work in excess of 40 hours per week.

d) Part of OPM's costs include such items as amortization of capital investments (for example, $8 million for phased-in automation of the program), recruiting and training of new investigators, "centrally funded" services (legal, public affairs, etc.), and similar costs not generally borne by retired Federal investigators.

e) State's $900 estimate does not include transcription services provided by the Department. Also, OPM's transcription costs are higher than State's because of our policy of providing a fully developed narrative record to the agency. State uses a summary reporting format.

f) Included in the price of every investigative product provided by OPM is a proportionate share of OPM's oversight, policy formulation, and central personnel security management costs.
On balance, therefore, we believe that the cost and quality of OPM's background investigations are competitive with those of State's investigations. Our own best estimate discloses an actual differential of less than $100 when true cost comparisons are made without even accounting for the expanded source coverage provided by OPM.

Q. The General Accounting Office entered into a memorandum of understanding with the Defense Investigative Service to conduct background investigations on a trial basis. During this pilot program, which ran from July 1, 1983, to July 1, 1984, randomly selected requests for investigations of GAO employees were given to OPM and DIS.

The results were that DIS completed 116 of 131 background investigations in an average completion time of 97 days.

OPM, on the other hand, completed only 59 of 123 background investigations in an average completion time of 218 days.

DIS charges GAO $800/case.

OPM's lowest charge was $1,450.

Would you please comment on this wide difference between DIS and OPM in, first, time to complete a background investigation and, secondly, in the comparative cost of each.

> GAO has been unwilling to share with us any of its comparisons, studies, or findings concerning the DIS/OPM "pilot program." Consequently, I will limit my response only to such information as OPM may have concerning our relative timeliness and cost standing vis-a-vis DIS.
>
> (a) Timeliness. As Mr. O'Brien's written statement delivered to the Subcommittee discloses, DIS had experienced a timeliness problem of almost 175 days in early 1982. By July 1983 and continuing through July 1984, DIS's backlog had declined to one of the lowest points reflected in the 6-year chart attached to Mr. O'Brien's statement. Between 1981 and 1983 DIS had increased its staff by almost 700 investigators, had placed a 3-year moratorium on periodic reinvestigation, and was assisted by over 100 OPM investigators detailed to DIS to help reduce its backlog. Hence, the 1-year GAO pilot project covered one of DIS's most propitious periods.
>
> The reverse was true for OPM. During the same period that DIS was experiencing 6-month delays in completing its BI's, OPM was completing its standard 75-day BI's in 57-68 days. It wasn't until early 1983 that OPM's workload began to increase precipitously, and was hitting new highs during the July 1983-July 1984 "pilot program" period. Hence, the GAO Study encompassed an atypical period both for DIS and OPM: while DIS was at its optimum timeliness point, OPM was at one of its worst. (See attached chart.)
>
> Even under these circumstances, however, OPM was able to complete its "expedite" cases in 68 days, and its normal 75-day cases in 190 days. GAO's record of 218 days was based on the lowest priority cases (i.e., "120 day" cases) requested of OPM.
>
> (b) Cost. In its 1979 study of Costs of Federal Personnel Security Investigations..., GAO found wide variance in the average cost of full-field investigations. Among the 11 major departments or agencies with investigative components, costs ranged from $208 to $1,058. According to the GAO Study:

> "OPM develops the most comprehensive (cost) data since it is required to recoup costs through reimbursement.... The average cost per investigation estimated by other agencies did not include comprehensive cost elements similar to those used by OPM. For example, DIS costs per investigation were estimated by using statistical studies and not by accumulating actual costs incurred. A DIS official said the estimates did not include such elements as DoD overhead, accrued leave, military retirement, automobile procurement, military and State Department personnel assistance overseas, FBI checks, and nonpayroll costs of supporting the military personnel assigned to DIS."

GAO found similar broad variances in "investigative scope," which it defined as -

> "the type and number of contacts with witnesses, record searches, letters of inquiry, and telephone interviews during the investigation. The scope of the investigations varies and thus employees are subject to inconsistent coverage resulting in possible overinvestigation or underinvestigation. Investigative scope also affects the scope and the amount of time involved in the investigation."

According to the most recent data available to us, the scope of OPM's standard background investigation ("BI") is more than twice as extensive as DIS's "BI" (30.2 vice 13.4 sources). Given the broad differences in both the quality and the costing of investigating services, it is not surprising that OPM charges considerably more than DIS for what may appear to be an identical "BI." In fact, under 5 U.S.C. 1304, we are required, unlike DIS, to assure that all our revolving fund services are accurately and fully costed. We do not know of a single instance of national security compromise resulting from individuals who had been investigated by OPM.

Q. A more recent test by GAO in November 1984 showed similar results. DIS completion time ranged from 57 to 97 days while OPM completion time ranged from 239 to 407 days. Likewise, DIS charged $500 for each case while OPM charged $1,375. It doesn't appear from this that OPM is really getting any better. When can you predict reducing your lag time in investigations?

Commencing in February 1985 and continuing to the present, OPM has already effected continuing improvements in timeliness. Based on the latest projections, we expect to return to our standard 35, 75, 120 day time-frame by October/-November of 1985 and reduce turn-around time even further to 30, 60, and 120 days by the end of this year.

Q. The Subcommittee sent letters to approximately 22 executive branch agencies asking for their respective comments concerning the efficiency and effectiveness of the government's personnel security program. Sixteen of these agencies responded with criticism of the investigative backlog at OPM and the delays the backlog has created in obtaining clearances for their personnel. For example:

> The Secretary of Transportation states "We are not satisfied with the time it takes OPM to conduct SBI, BI and NACI investigations. Delays require frequent pre-appointment waivers prior to completion of the required investigations."
>
> Ford B. Ford, Under Secretary of Labor, stated that the "turn-around time is about 120 days on cases for which we request expedition within 35 days. The delay in filling key jobs renders a hardship with regard to DoL programs."
>
> James C. Sanders, Administrator of the Small Business Administration, told us "We are not satisfied with these turn around times, particularly with regard to full field investigations. Because there is an 8 month turn around time for 120 day investigations, we have been forced to choose between delaying the filling of ... positions, increasing the use of expedited investigations at a great increase in cost, or appointing employees prior to completion of the investigation."

A draft statement of one federal agency stated that "the only consistent step taken by OPM over the years has been to raise the price charged for an investigation. ...OPM management officials were promoting the idea that with new forms, a new investigative format, and additional investigators, the backlog of cases would be reduced to a manageable level.... Security officials realized that the OPM plan was unrealistic and could not succeed. As a result, our frustrations grow deeper."

Will you comment on this please?

> We have already addressed timeliness and backlog problems both in the written statement and in the various other questions and answers provided by and to the Subcommittee. For the record, however, we would like to correct several points made by the various respondents to your inquiries: (1) Turn-around time on 35 day BI's has averaged 66 days--not 120; (2) although we were forced to increase prices in 1982 to eliminate the $6.5 million deficit carried over from the prior Administration, we actually reduced prices in February 1984; and (3) despite the fact that the workload began increasing in 1983, the timeliness problem did not become significant until the latter half of 1983.

We have taken a number of measures to control and eliminate the problem. These measures have already begun to produce the desired results. During the last 3 months the backlog has been reduced by 10 percent and we expect large and continuing declines over the next 6 months with resultant improvement in timeliness. We project an average 75-80 day turn-around by the end of the current fiscal year, and a 60-75 day turn-around by October or November of this year.

No other agency, to our knowledge, can claim a similar record of success against adverse circumstances, without degradation in quality, suspension of other investigative responsibilities, or increase in cost. Nor has any other agency developed and implemented systemic management measures to preclude future recurrence of longstanding, cyclical timeliness problems.

Q. It is our understanding that due to the Privacy Act of 1974 and the fear of harmful litigation, only approximately 63% of American corporations provide OPM with complete information. I believe your agency has prepared a list of those non-cooperating corporations which I will ask you to furnish to this Subcommittee for introduction into the Record. Additionally, do you have any suggestions to help remedy this problem?

The attached listing of employing institutions is neither comprehensive nor dispositive of the problems we have experienced in securing employment information. It was assembled locally to provide management with some insight into the scope of the problem, but should not be viewed as adequate per se, or even as reflective of national corporate policies.

While there are a number of possible solutions to this problem, one readily available partial solution would be to provide for standard language in all Federal contracts, loans, and grants requiring that all recipients of public moneys provide employment information to Federal investigators.

Q. Additionally, I believe your agency has prepared a list of non-cooperating law enforcement agencies. Would you please provide us with that list and briefly explain what the problem is with these law enforcement agencies? Additionally, do you have any suggestions to remedy this problem?

The attached list delineates some of the difficulties we have encountered in seeking access to local arrest and conviction records. They include the following:

1. Privacy Act considerations;

2. Dissemination limited to criminal justice or law enforcement agencies;
3. Inability to provide NCIC number;
4. Unique identifying or release requirements;
5. "Policy" considerations;
6. Resource limitations;
7. Restrictive state statutes;
8. Fee requirements; and
9. Private sentiments by police officials.

The major part of OPM's, DIS's, and other investigative agencies' problems in gaining access to local law enforcement information would be solved if these agencies were recognized as involved in enforcement of national security laws and were assigned the use of an NCIC number. Some additional clarification of public or private liability under the Privacy Act for both local law enforcement agencies and employing institutions would help in removal of the remaining obstacles.

The Department of Justice, in consultation with other Federal, State, and local jurisdictions, is now reviewing the manner in which criminal justice data are shared and access to those data. A favorable decision for OPM and other personnel investigations agencies in this forum would move us much closer towards solving this problem.

Q. In January 1984 the Office of Personnel Management issued Basic Installment 311 to replace existing suitability guidelines for the Federal Personnel Manual. The Subcommittee has received information from several executive branch agencies which is highly critical of 311. We have documentation stating that 311 was drafted and issued without any coordination with the executive branch agencies and, in particular, the NSDD-84 study group chaired by Justice. I want to read some agency comments regarding 311.

"OPM's recent publication of the revised Federal Personnel Manuals in January 1984 was done in haste with the apparent motive to defeat possible recommendations from an interagency task group studying the personnel security program."

"At a time when budgets and staffs are being reduced in the civilian departments/agencies, OPM would have personnel security officers be responsible for additional tasks requiring increased staffing to properly implement the provisions of revised Federal Personnel Manuals."

"A complicated series of computation forms must be completed to determine which investigation applies to two levels of non-critical-sensitive positions. Expanding the required investigations in this manner will increase the investigative time of OPM and other investigative agencies, impose additional delays, elevate costs and require increased personnel security staffs."

"Basic Installment 311 is in essential conflict with the options recommended by the NSDD-84 group. It improperly merges responsibility for personnel suitability-personnel security determinations. Such merging will only serve to further aggravate the situation in which courts intrude into Executive Branch prerogatives concerning authority to make personnel security decisions."

Was Basic Installment 311 a product of the NSDD-84 interagency group?

Were the members of the NSDD-84 interagency group advised on 311? Did they have any input?

Was there coordination with the executive branch agencies in drawing up 311?

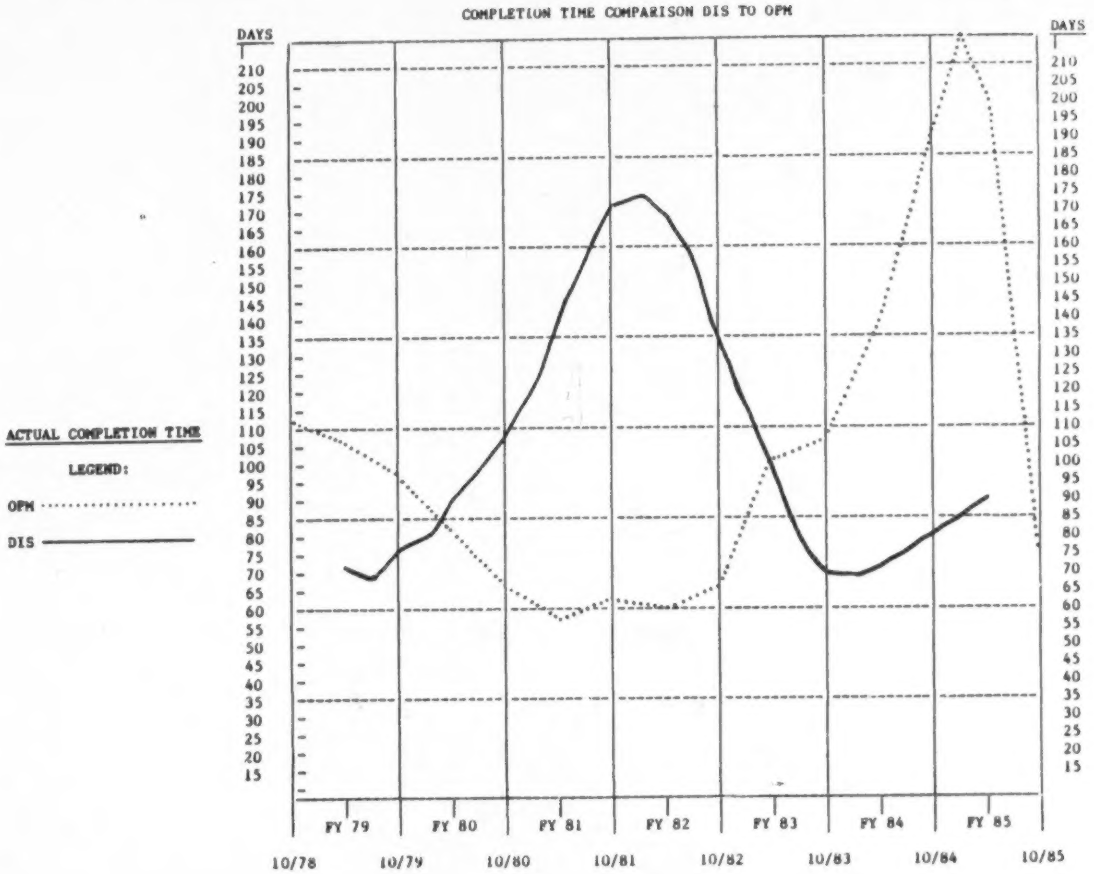
Is 311 acceptable to the agencies? Are the agencies implementing it?

> Generally speaking, we have not experienced widespread, adverse reaction to OPM's guidance as set forth in FPM Basic Installment 311. It is also our understanding that of the 22 inquiries transmitted by the Senate Subcommittee, only 2 agency responses -- Treasury's and FCC's -- were critical.
>
> The FPM issuance is guidance to agencies, and, as all guidance, is issued under authority inherent in OPM as a central management agency. Nevertheless, long before we issued FPM Installment 311 in January 1984, we consulted extensively with agencies on the problems addressed in the issuance. We met with DoD, Justice, Treasury, and a number of other major agencies throughout 1980 and 1981 to conduct an "Interagency Study on Implementation of GAO Recommendations." This study and the resulting recommendations were endorsed in whole or in part by over 90 percent of all agencies, including the General Accounting Office. We ultimately incorporated many of the recommendations and clarifications into the 311 Series, including modifications resulting from the NSDD-84 interagency consultative process.
>
> After we issued Basic Installment 311, we conducted an extensive series of briefings, seminars, and workshops to explain the Installment and resolve problems. Over 85 such briefings were held. In March 1984, we conducted a telephone survey to identify specific problems by pointing out the flexibility and discretionary latitude provided by the 311 Series, and OPM will provide some additional FPM guidance to that effect.

Thus, it is evident that extensive consultation both preceded and followed the issuance of Basic Installment 311. This was especially the case in the course of the NSDD-84 consultative process. While the precise details of Basic Installment 311 were undergoing review at OPM, numerous changes were made to assure consistency with consensus sentiment evolving from the NSDD-84 process. Of particular note are the findings and recommendations that suitability issues should be kept separate from security, and that OPM has sole and exclusive responsibility over suitability matters. To the extent that the NSDD-84 interagency group members had participated in the earlier Task Force Study, most of their concerns and interests had already been taken into consideration. But it was not a product of the NSDD-84 Working Group. There is, in fact, no inconsistency between the security based NSDD-84 Study and OPM's guidance in Basic Installment 311.

Basic Installment 311 has been widely recognized as a significant improvement over the out-dated patchwork of confusing guidance it replaced. With the exception of DoD and Treasury, virtually all agencies have begun upgrading their programs to conform to the more precise guidance offered under 311. Some agencies are reporting declines in costs resulting from more accurate position sensitivity designation. Others, particularly those agencies that have very limited "access" requirements, are appreciative of the flexibility and the sounder legal footing provided by 311.

The occasional critical comment concerning OPM's FPM issuance is fairly commonplace whenever the agency attempts to recodify and republish existing guidelines.



COMPLETION TIME COMPARISON DIS TO OPM

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTIONS
CH	Chicago, IL	IBM	Company policy to destroy records after one year.
	Deerfield, IL	Walgreen Drug	Verify name and dates only. No personals no leads.
	Cincinnati, OH	Proctor and Gamble	" " " " " " "
SL	Dubuque, IA	John Deere	Record search only. No personals or leads.
	Mason City, IA	A.C. Neilson	Dates of employment and title. No personal or leads.
	Lenexa, KS	Coca Cola	Provide dates only. No personals or leads.
	Omaha, NE	Mutual of Omaha	No~~thing~~ information given out.
	Overland Park, KS	Wausau Insurance	Verify name and dates only. No personals or leads.
	Overland Park, KS	Traveler's Insurance	Record search only. No personals or leads.
	Kansas City, MO	St.Lukes Hospital	" " " " " " "
	Topeka, KS	Josten's Inc.	" " " " " " "
	St. Louis, MO	Famous-Barr Dept. Store	" " " " " " "
DA	Dallas, TX	EDS (Electronic Data Systems)	Record over the telephone only. No personals or leads.
	Dallas, TX	Texas Instruments	Record search only. No personals or leads.
	Dallas, TX	Dallas Times-Herald	Verify name and dates only. No personals or leads.
	Dallas, TX	Binswanger Glass	No~~thing~~ information given out.

EMPLPOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTIONS
DA	Wichita Falls, TX	Sprange Electric	Record search only. No personals or leads.
	Iowa Park, TX	Cryovac, Inc.	" " " " " " "
	Dallas, TX	NCR	" " " " " " "
	Dallas, TX	Neiman Marcus Dept. Store	Verify name and dates only. No personals or leads.
	Dallas, TX	InterFirst Bank	Record search only. No personals or leads.
	Dallas, TX	Texas Federal S&L	" " " " " " "
	Irving, TX	L.D. Brinkman	" " " " " " "
	Dallas, TX	Information Processing Corp.	" " " " " " "
	Houston, TX	Houston Power and Light	" " " " " " "
	Houston, TX	Southwestern Bell	" " " " " " "
	Tulsa, OK	Public Services Co. of Oklahoma	" " " " " " "
	Tulsa, OK	Warren Petroleum (subsidiary, Gulf Oil)	" " " " " " "
	Albuquerque, NM	GTE Lenkirk	" " " " " " "
	Albuquerque, NM	Sperry Flight Systems	" " " " " " "
	Albuquerque, NM	Digital Inc.	" " " " " " "
	Houston, TX	Slumbuger, Inc.	" " " " " " ".

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTIONS
DA	Houston, TX	Bechtel, Inc.	Record search only. No personals or leads.
	Amarillo, TX	Pantex	Will co-operate, however there is no place set aside for interviews. People are called away from their work stations and waiting for source availability affects timeliness.
	Borger, TX	Phillips Petroleum	Provide record and leads. Do not permit interviews on site. ✓
	Amarillo, TX	ASARCO	Record search only. No personals or leads.
	Lubbock, TX	Texas Instruments	Verify name and dates only. No personals or leads.
	Sante Fe, NM	Eberline Instruments	Record search only. No personals or leads.
PH	Wilmington, DE	Dupont	Verify record information. Permit personal interviews, but must go through legal department, resulting in 2 weeks delay.
	Philadelphia, PA	First Penn Bank	Verify name and dates only. No personals or leads.
	Three Mile Island, PA.	General Public Utility	Will provide record information when furnished a release and a letter detail-the information requested. Procedure not timely. No personals or leads.
	Trexlertown, PA	Air Product and Chemical, Inc.	Record search only. No personals or leads.
	Baltimore, MD	J.C. Penneys	- - - - - - -
	Baltimore, MD	Chessie R.R.	- - - - - - -

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTIONS
PH	Baltimore, MD	Hutzler's Dept. Store	Record search only. No personals or leads.
	Martinsburg, WV	Bethlehem Steel	" " " " " " "
	Richmond, VA	Thalhimers Dept. Store	Verify name and dates only. No personals or leads.
	Richmond, VA	Sovran Bank	" " " " " " "
	Richmond, VA	C&P Telephone Co.	" " " " " " "
BN	Boston, MA	John Hancock	Verify name and dates only. No personals or leads.
	Boston, MA	Prudential	" " " " " " "
	Boston, MA	Liberty Mutual	" " " " " " "
	Hartford, CT	Traveler's Insurance	" " " " " " "
	Blumfield, CT	Sigma General Life	" " " " " " "
	Hartford, CT	Hartford Insurance Group	" " " " " " "
	Region wide	Banking institutions	" " " " " " "
	Sta~~p~~mford, CT	Pitney-Bowes	Record search only. No personals or leads.
	Maynard, MA	Digital, Inc.	" " " " " " "
	Attleboro, MA	Texas Instruments	" " " " " " "
	Springfield, MA	Monsanto	" " " " " " "

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTIONS
NY	NY,NY	CBS	Verify name and dates only. No personals or leads.
	NY,NY	Merrill Lynch	" " " " " " "
	NY,NY	Time, Inc.	Record search only. No personals or leads.
	NY,NY	Time Magazine	" " " " " " "
	NY,NY	ASCAP	Verify name and dates only. No personals or leads.
	NY,NY	Macy's	Record search only. No personals or leads.
	NY,NY	Chemical Bank	" " " " " " "
	NY,NY	Alexander Dept. Stores	" " " " " " "
	NY,NY	Columbia Presbyterian Hospital	" " " " " " "
	Uniondale, NY	Marriott Hotels	" " " " " " "
	NY,NY	Cosmopolitan Magazine	Letter Requesting Record information only. No personals or leads.
	San Juan, PR	Banco de Ponce	Record search only. No personals or leads.
	Livington, NY	Continental Bank	Verify names and dates only. No personals or leads.
	Albany, NY	State Bank of Albany	" " " " " " "
	Albany, NY	Albany Medical Center	" " " " " " "
	~~Forkedriver~~, NJ Forked River	Jersey Central Power and Light Co.	Record search only. No personals or leads.

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTION
AT	Lexington, KY	Square D Company	Verify dates of employment only. No leads or personals.
	Memphis, TN	Methodist Hospital	Requests release less than 30 days old. No personals no leads.
	Columbia, SC	Southern Bell	Nothing.
	Jacksonville, FL	Prudential Insurance	Record search only. No personals no leads.
	Mobile, AL	International Paper	" " " " " " "
	Gibson, MS	Bechtel Corp.	Usually record search, but sometimes nothing at all. No personals no leads.
	Tampa, FL	A.C. Neilson	Nothing.
	Tampa, FL	Photomat	Record search only. No personals no leads.
	Aikin, SC	Aikin Electric Corp.	Leads only, no record of any kind.
	Augusta, GA	Allstate Insurance	Nothing.
	Augusta, GA	Augusta Newsprint	Nothing.
	Blankville, SC	Ducane Heating	Record search only. No personals no leads.
	Aikin, SC	FNC Company	" " " " " " "
	Augusta, GA	Georgian Railwood Bank	" " " " " " "
	Augusta, GA	Kentucky Fried Chicken	" " " " " " "
	Beach Island, SC	Kimberly Clark	" " " " " " "
	Augusta, GA	Murray Biscuit	" " " " " " "

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTIONS
AT	Augusta, GA	Babcock/Wilcox	Record search only. No personals or leads.
	Barnwell, SC	Burlington Distributers	" " " " " " "
	Augusta, GA	Citizins & Sothrn Bank	" " " " " " "
	Augusta, GA	Columbia Nitrogen	" " " " " " "
	Willston, SC	DAYCO, Inc	" " " " " " "
	Aikin, SC	Pepperidge Farm	" " " " " " "
	Augusta, GA	Proctor & Gamble	" " " " " " "
	Augusta, GA	Searle Corp.	" " " " " " "
	Denmark, SC	Sunbeam Corp.	" " " " " " "
	Montgomery, GA	W.F. Hall Printing	" " " " " " "
IWD	Rockville, MD	EDS	Security office is cooperative. Personnel office provides record, but no personals
	Fairfax, VA	McDonald's Corp.	Verify name and dates only. No personals or leads.
	Arlington, VA	American Gas Assn.	" " " " " " "
	Oakton, VA	AT&T	" " " " " " "
	Washington, DC	C&P Telephone Co.	" " " " " " "
	Washington, DC	Banks in general	Record search only. No personals or leads.
	Washington, DC	Blue Cross/Blue Shield	" " " " " " "
	DC Area	GEICO	" " " " " " "

EMPLOYMENT ACCESS RESTRICTIONS

REGION	CITY/STATE	COMPANY	RESTRICTION
IWD	DC Area	Woodward & Lothrop, Hecht's, Garfinkle's, Bloomingdale's, Montgomery Wards, Giant, Safeway, Toys R' Us	Record search only. No personals no leads.
	Washington, DC	Heritage Foundation	Record search only. No personals no leads.
	Washington, DC	IBM	Record search and leads. No personals.
	DC Area and N. Virginia	Law Enforcement Agencies	PD's do not conduct searchs, and courts only provide limited backup. Records are kept in docket books, filed alphabetically on a daily basis, so the searches are "hit or miss" at best.
	Alexandria, VA	Peoples Drug Stores	Verify name and dates. No personals/leads
	Rockville, MD	NUS	" " " " " " "
	Gaithersburg, MD	Bechtel Corp.	" " " " " " "
	Beltsville, MD	District Photo	" " " " " " "
	Washington, DC	House Disbursing Office	Record search only. No personals or leads.
	Washington, DC	Senate Personnel Office	" " " " " " "
	Washington, DC	USIA Security Office	Are called and are told they have a security file. 2 weeks later they still don't have the file.
	Washington, DC	National Academy of Sciences	Only cofirm name and dates. No personals or leads.

EMPLOYMENT ACCESS RESTRICTIONS

preliminary study [illegible]

REGION	CITY/STATE	COMPANY	RESTRICTION
OPI/IOD	Boyers, PA	On the basis of a limited survey of 450 NACI cases, the following employment response/access information was recieved: 975 Total employers contacted (2.16 per case). 703 (72%) Total employer responses recieved (1.56 per case), at approximately 49 days from date of case scheduling. 611 (87%) of responses received were completed. 62 (8.8%) responses received restricted amount of information. ✓ 30 (4.2%) responses returned as "Undeliverable." Overall employer contact statistics: 28% Fail to respond to inquiries. 6% Respond to inquiries but restrict information. 3% Inquiries returned "Undeliverable." 63% Inquiries returned with information provided.	

LAW ENFORCEMENT JURISDICTIONS NOT RESPONDING TO PERSONAL VISITS

ATLANTA REGION

North Carolina Division of Motor Vehicles	Fee of $7.00 per record search.
South Carolina Division of Motor Vehicles	Fee of $2.00 per record search.

BOSTON REGION

Massachusetts Board of Probation	Fee of $3.00 per record search. Will only provide conviction data.
Providence, RI City PD	Personal policy of Chief of Police. (No real problem since records can be obtained from State Police.)
Massachusetts State PD Cambridge, MA City PD Waltham, MA City PD Arlington, MA City PD Sharon, MA City PD	Denied or restricted access to records. (Interpretation that OPM only has access to records through MA Board of Probation.)

CHICAGO REGION

Illinois State Dept. of Law Enforcement	Primary - Lack of resources. Secondary - State law/policy - must be criminal justice at least for arrest data.
Schaumburg, IL City PD	Follows State Dept.'s policy.
Park Forest, IL City PD	Privacy Act (will release "No Record" only).
Niles, IL City PD	Longstanding policy - Privacy Act and other.
Evansville, IN City PD	Fee of $3.00 for record search. ($7.00 fee if copy of arrest record provided.)

DALLAS REGION

Tarrant County Sheriff's Dept., TX Garland, TX City PD De Soto, TX City PD Mesquite, TX City PD Lewisville, TX City PD Plano, TX City PD Duncanville, TX City PD Tyler, TX City PD Fort Worth, TX City PD (unless contacted after the day shift leaves.)	All require NCIC #. OPM not criminal justice.

DENVER REGION

Wyoming State PD Cheyenne, WY City PD Casper, WY City PD Rock Springs, WY City PD Sheridan, WY City PD	All require NCIC #. State law/policy.

NEW YORK REGION

New York State Police	Will search only if indication of arrest - lack of resources. No real problem since all routine checks are made at local level.
NY State Division of Criminal Justice Services (Central repository for all state arrest data)	OPM not a criminal justice agency. Need NCIC #. (Coverage obtained thru local law enforcement checks.)

PHILADELPHIA REGION

Virginia State PD	Fee of $5.00 for record search. Race and sex identifiers required for search.
Richmond, VA City PD	Race and sex identifiers required for search. Will only provide conviction data.
General District Court #1 (Richmond) Norfolk, VA District Court	Both require specific trial date to get records.
Norfolk, VA City PD	Must be criminal justice. Otherwise, will only provide Class 3 & 4 misdemeanors.
Hampton, VA City PD Virginia Beach, VA PD	Both will only provide conviction data.
Newport News, VA City PD	Fee of $5.00 for record search. Will only provide class 3 & 4 misdemeanors.
Philadelphia, PA City PD	Fee of $75.00 for record search.
Delaware (all jurisdictions)	State law/policy - Must be criminal justice.

SEATTLE REGION

Washington State Police Island County Sheriff, Coupeville, WA Renton, WA City PD	State law - all require must be criminal justice.
Seattle, WA City PD	Fee of $6.00 per record search. More if there is a record.
King County Sheriff, Seattle, WA	Fee of $6.00 per record search. Provides conviction data only.

Spokane, WA City PD	City PD's release must be signed by subject and notarized for conviction data. No arrest data - must be criminal justice by State law.
Oregon State PD	State law - must be certified by Governor - criteria for certification is criminal justice.
Portland, OR City PD	Conviction data only provided. Must be certified by Governor for arrest data.

SAN FRANCISCO REGION

California State Investigation and Identification Bureau	Requires fee of $6.50 and 2 finger print cards.
Alameda County, CA Sheriff's Office	Requires fee of $10.00 for list containing 1 to 20 names and $10.00 for every record furnished.
Sacramento, CA City PD Oakland, CA City PD Pleasanton, CA City PD Los Gatos, CA City PD Culver City, CA PD	All lack resources - Staff will not let OPM conduct record search.
Inglewood, CA City PD Gardenia, CA City PD Hawthorne, CA City PD San Bernadino, CA City PD Menlo Park, CA City PD Walnut Creek, CA City PD Richmond, CA City PD Daly City, CA PD	OPM not a law enforcement agency.
Arizona Dept. of Public Safety Phoenix, AZ City PD Flagstaff, AZ City PD Prescott, AZ City PD Willcox, AZ City PD Pima County, AZ Sheriff's Office	State Law - OPM not criminal justice.
North Las Vegas, NV City PD	Fee of $2.00 per page for arrest data.

ST. LOUIS REGION

Regional Justice Information Service (covers MO jurisdictions in the St. Louis Metropolitan area.)	Fee for record search.(Fee not known yet - will be approximately $1.50 per record search.)

WASHINGTON DIVISION

Alexandria, VA City PD Arlington County, VA PD Fairfax County, VA PD Prince William, VA PD	All require race and sex identifiers for record search. Otherwise, will only provide Class 3 & 4 misdemeanors.

LAW ENFORCEMENT AUTHORITIES NOT RESPONDING TO VOUCHERS

AL: Marshall Space Flight Center
AK: Do Not Voucher
AZ: Tucson, Phoenix, Tempe
CA: See List
CO: Denver, Durango, Colorado Springs, Aurora
DE: Do Not Voucher
DC: Do Not Voucher
FL: See List
HI: Do Not Voucher
IL: Do Not Voucher
IN: Evansville
IA: Cedar Rapids, Dubuque
KS: Kansas City
KY: Morehead
LA: Metairie, Monroe
MA: Do Not Voucher
MI: Detroit
MN: Do Not Voucher
NE: Lincoln, Omaha
NH: Dover
NJ: Newark, West Trenton
NM: Alamagordo, Farmington, Las Cruces
NY: Do Not Voucher
OH: Cincinnati, Cleveland, Eastlake, Springfield, Toledo, Youngstown
OK: Lawton, Norman
OR: Eugene, Salem
SC: Georgetown
TN: Chattanooga
TX: See List
VA: See List
WA: Seattle, Spokane, Takoma
WV: Do Not Voucher
WI: Wauwatosa
Guam: Do Not Voucher
Canal Zone: Do Not Voucher

CALIFORNIA

Alhambra *
Anaheim *
Arleta *
Barstow *
Bel Air *
Bellflower *
Campbell *
Carmichael *
Castro Valley *
Commerce *
Corona *
Culver City *
Davis *
Downey *
East Los Angeles *
El Centro *
Foster City *
Fresno *
Fullerton *

Highland *
La Jolla *
Lakeview Terrace *
Lakewood *
Lancaster *
Long Beach *
Los Angeles *
Mar Vista *
Marina Del Rey *
Merced *
Millbrae *
Napa *
North Highlands *
Northridge *
Novato *
Oakland *
Oxnard *
Pacific Grove *
Palms *
Palm Springs *
Panorama City *
Pasadena *
Petaluma *
Pico Rivera *
Redondo Beach *
Redwood City *
Richmond *
Riverside *
Sacramento *
San Diego *
San Fernando *
San Francisco *

San Lorenzo *
San Mateo *
San Pablo *
San Pedro *
Sanford *
Santa Ana *
Santa Maria *
Stockton *
Studio City *
Sun Valley *
Sylmar *
Terminal Island *
Tracy *
Tujunga *
Tulare *
Tuluca Lake *
Tumunga *
Tustin *
Upland *
Vacaville *
VENICE -
Ventura
Walnut Creek
West Hollywood
Wilmington
Yucaipa

FLORIDA

Bal Harbour Village	*
Bay Harbor Islands	*
Biscayne Park	*
Coral Gables	*
El Portal	*
Florida City	*
Golden Beach	*
Hialeah	*
Hialeah Gardens	*
Homestead	*
Indian Creek Village	*
Key Biscayne	*
Medley	*
Miami	*
Miami Beach	*
Miami Shores	*
Miami Springs	*
North Bay Village	*
North Miami	*
North Miami Beach	*
Opa-Locka	*
South Miami	*
Surfside	*
Sweetwater	*
Virginia Gardens	*
West Miami	*

TEXAS

Abilene	*
Baytown	*
Beaumont	*
Denton	*
Duncanville	*
El Paso	*
Garland	*
Grand Prairie	*
Houston	*
Hurst	*
Irving	*
Mesquite	*
Nederland	*
Plano	*
Richardson	*
Temple	*

VIRGINIA

Alexandria
Arlington
Berkeley
Bowers Hill
Canden Mills
Chesapeake
Churchland
Cradock
Debree
Deep Creek
Fentress
Fleet
Great Bridge
Hampton Roads
Herndon
Hickory
Milan
Norfolk
Norville
Ocean View
Poquoson
Portlock
Richmond
St. Bridge
Semondale
Staunton
Suffolk

Senator **Nunn**. Mr. Dalinsky, could you hold up your right hand? We swear all witnesses before the subcommittee.

Do you swear the testimony you will give before the subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. **Dalinsky**. I do.

Senator **Nunn**. Thank you, sir.

TESTIMONY OF A. BARRY DALINSKY, DEPUTY DIRECTOR OF SECURITY DIVISION, DEPARTMENT OF ENERGY

Mr. **Dalinsky**. Mr. Chairman and members of the subcommittee, I am very pleased to be here today with Mr. John Miller, who is Chief of our Personnel Clearance Branch, to discuss with you Department of Energy's personnel security program.

I have written testimony and attachments, and we request that this testimony be accepted by the subcommittee for inclusion into the record of these proceedings.[1]

Senator **Nunn**. Without objection, your full written testimony will be placed in the record. We appreciate that very much. I have read all of your testimony, believe it or not. I would appreciate very much if you would summarize it this morning. We had an unexpected Intelligence Committee hearing come up. Although I definitely will be late, I would like to get there before the conclusion.

Mr. **Dalinsky**. I thought that, in the interest of time, I would keep my remarks brief and just take a few minutes with my opening remarks, and if you have any questions, of course, I will be pleased to answer those.

The Department of Energy has the largest personnel security program of any civilian agency or department in the executive branch in terms of the number of people possessing active clearances and number of clearance requests processed annually.

Our written testimony addresses a number of aspects of our personnel security program, including its legal basis, relevant statistics, administrative due process procedures, and reinvestigation activities.

The foundation of our program rests on the following principles that have been instrumental in shaping our current policies and procedures:

First, when dealing with individuals and questions of access, there is no such thing to us as an individual who presents no risk. We make adjudications from the standpoint of whether or not an individual is an acceptable or unacceptable risk.

Second, access is access. By that I mean that we have one clearance criteria and it applies for an adjudication no matter whether an individual is being processed for access to top secret, secret, or confidential information.

Third, the personnel security program is not a stand-alone activity, and we do not view it as such. We look at our program activities from the context of our overall security objectives and how it fits in with physical protection, operational security, and other parts of the effort.

---

[1] Mr. Dalinsky's prepared statement follows his testimony. The attachments referred to may be found on p. 783.

Fourth, our personnel security program is not totally centralized or decentralized. It's a combination of the two approaches that we have developed over many years, and we feel best fits our way of doing business at the Department.

Fifth, final determinations in derogatory cases must be made in favor of national security when any doubt exists, but we assure that the individual involved is always afforded administrative due process procedures.

Sixth, the spectrum of threat from individuals is not limited to espionage. Such threats also encompass sabotage, theft, or diversion—in the Department of Energy—of special nuclear material, protection of Government property, and one thing we seldom discuss but also give consideration to is the protection of our employees and contractors in their work environment.

Seventh, our policy has always been the fewer clearances, the better. As the number of cleared individuals decreases, so does the probability of an occurrence of an insider malevolent act or unauthorized disclosure of classified information.

Eighth, any program should not be static but one that is proactive and should remain flexible to adjust to changing threats to the national security. Any program that deals with individuals needs constant review, modification, oversight, management support, and training and retraining of personnel.

And, ninth and last, periodic reinvestigations of cleared personnel must be accomplished. The most serious problems and the most attractive targets for hostile intelligence services will be presented by people on the inside and not by people on the outside.

No matter how good a personnel security program is, and we believe the Department of Energy does have a very good program, occasionally mistakes and questionable adjudications and determinations may be rendered. It's not the fault of the system or the procedures, but rather the fault of the individuals responsible for implementation of the procedures.

The matter of Takis Veliotis has been raised, and I think this is an excellent example of how failure to follow established procedures can lead to a questionable adjudication. It is also an excellent example of why the Department of Energy has stringent requirements for processing clearance applications for foreign nationals and why there are only 4 cleared foreign nationals out of 201,000——

Senator **Nunn** [interposing]. While you are on that point, can you tell us why those procedures were not followed in the Veliotis case?

Mr. **Dalinsky**. Specifically, information was not obtained from Veliotis as required on a Form AEC-15. More information for the investigative agencies, in this case the FBI, to do its work.

Second, an interview with the individual was not done and should have been done according to our requirements.

Senator **Nunn**. And these two responsibilities were FBI?

Mr. **Dalinsky**. No; the responsibility for conducting the investigation was the FBI's. The responsibility for conducting the interview was the Department of Energy's.

Senator **Nunn**. I see. So you say both were at fault?

Mr. DALINSKY. No; I'm saying the Department was at fault because we should have provided the additional information to the FBI for them to do the investigation. That is our requirement on processing foreign nationals.

Senator NUNN. So you are saying the primary fault in the Veliotis case investigation was the responsibility of or failure in the Department of Energy?

Mr. DALINSKY. I am saying that if we had followed the requirements that we have in place, and had in place at that time, the result might have been a different adjudication of that case than what we had, which was a granting of a clearance.

In other words, the technical requirements were not followed.

Senator NUNN. You don't fault the investigation of the FBI; you don't have any critique of that in the Veliotis case?

Mr. DALINSKY. No; I don't.

Senator NUNN. Thank you.

Mr. DALINSKY. Personnel security program problems that the DOE faces daily are no different than the problems faced by all members of the U.S. intelligence and security communities. Some of the problems, of course, we deal with are the continuing inability to obtain adequate information about an individual for use in adjudications. I think that matter has been gone over and probably will be addressed even more in these hearings.

We have to resist pressures to reduce investigative coverage as a response mechanism to increasing costs and investigative times. We have to resist internal pressures to use the waiver process to permit individuals access to classified information or employment before investigation is completed or adjudicated.

Obtaining and maintaining adequate staff and trained professionals, be they investigators or adjudicators, of course, is a continual problem. Sharing information in derogatory cases with other concerned agencies is something we always have to constantly be on the alert for and, last, assuring consistency in the implementation of program requirements and standards. Again, the last one, I think, applies to the Veliotis case.

We believe that these and other problems must be addressed and resolved in the interest of national security and for the Government's personnel security programs to maintain a degree of effectiveness, reliability, and integrity.

Again, I have tried to keep my remarks as brief as possible, and I will be glad to entertain any questions from the subcommittee.

Senator NUNN. Thank you very much. We appreciate you being here and appreciate that very concise summary.

What procedures do we have in effect, or maybe the word "procedures" is not correct. Would you have confidence that another case like Veliotis would be handled differently today in the Department of Energy?

Mr. DALINSKY. I feel very confident that it would for the following reasons:

There is a lot more awareness in all areas of the Department, in all management levels, of the importance of the personnel security activities. We have entered into a program of training our personnel, a program we did not have before, and a program of field oversight; that is of going out and visiting the field and checking on how the personnel security activities are conducted out at those sites.

Again, in the Department of Energy, clearances are granted not only at DOE headquarters but in each of our 10 field offices. So each of those field offices under the field office manager has the authority to adjudicate and grant clearances.

Senator NUNN. Are you satisfied with the Office of Personnel Management's handling of security investigations for your agency at this point in time?

Mr. DALINSKY. Yes, Senator, we are. We, by law, set the scope and extent of investigation under section 145 of the Atomic Energy Act of 1954 as amended. If we were not satisfied, or felt that scope and extent should be revised, we have the authority by law, if I may use the word, to order OPM to give us a product that we desire.

Senator NUNN. So you set the quality standards by your specifications?

Mr. DALINSKY. That's correct.

Senator NUNN. And they comply with those?

Mr. DALINSKY. That's correct.

Senator NUNN. What you require is not necessarily what other agencies require; it could be different?

Mr. DALINSKY. It could be.

Senator NUNN. Have you had occasion to examine the requirements you have in your agency a compared to Defense Investigative Service requirements?

Mr. DALINSKY. We, ourselves, have not done a comparison study.

Senator NUNN. Have you looked at any of the cost factors involved for comparing OPM's investigation with DIS?

Mr. DALINSKY. No; but that fact was brought forward to us in the Grace Commission Report when the recommendation was made for the Department of Energy to utilize the Defense Investigative Service because of the difference in investigative costs.

Senator NUNN. And what was your conclusion from that recommendation?

Mr. DALINSKY. The recommendation really went a little bit beyond that of the DOE using the Defense Investigative Service to conduct our background investigations. Of course, that would have to be changed by law if, in fact, we did that. The primary recommendation was that the DOE should become a Defense Industrial Security Program user agency.

In our review of that particular recommendation, we found that it was not feasible to implement it at the department; that is, we could not become a DISP user agency because that would mean that not only would background investigations be done by DIS, but also our whole security program, protection of our nuclear facilities, would come under the DIS program.

We did contact and meet with officials from the Office of the Secretary of Defense for Policy to discuss the possibility and feasibility of the Department of Energy utilizing the Defense Investigative Service. We prepared a very extensive package for them which laid out what type of service we wanted, what scope we wanted for our investigations, and all of the other types of peripheral services we normally are afforded by OPM, and the other things we would like also.

We gave all that to them and asked them to give us a cost-per-case estimate for that type of service. About 6 months later we had another meeting but were not provided that information. At that meeting, we were again asked to consider becoming a DISP user agency. After that meeting, we went back to the Department of Defense in writing and stated that we thought the meetings should come to a close because we really had not been provided the information we had asked for, which was an indication as to what the cost-per-case would be by our standards.

Senator NUNN. You never did get that information?

Mr. DALINSKY. We never got a bottom-line price, so we really had no way—and there was nothing in the Grace Commission Report to substantiate that figure, so we said if the DOE goes with this recommendation, and we get the service that we want, what would it really cost us? We were never really told.

Senator NUNN. Did you all participate in this task force we have been talking about this morning? Did Department of Energy have someone on that?

Mr. DALINSKY. On the—which?

Senator NUNN. The NSDD-84 Task Force on the whole security problem. Did the Energy Department participate?

Mr. DALINSKY. No one that I am aware of, but I could go back and check and let you know that information.

Senator NUNN. If you could furnish it for the record.[1] Do you have changes in the law in this overall security area from the perspective of the Department of Energy that you would recommend? Changes in the law?

Mr. DALINSKY. Any type of law?

Senator NUNN. Any type of law that pertains to this problem, relates to this problem. [Laughter.]

Mr. DALINSKY. Well, we did have some problem with the Privacy Act, but I don't know if that relates to this particular problem or not.

Senator NUNN. I understand it does. Have you had any problem with State and local agencies furnishing material?

Mr. DALINSKY. The Department of Energy is not an investigative agency, so we utilize OPM and the FBI law to conduct our investigations.

Senator NUNN. Right.

Mr. DALINSKY. It has been obvious to us that the investigative agencies, particularly OPM because they are not designated as a law enforcement agency, have had problems procuring information, particularly criminal information from State and local law enforcement authorities. I think that if some sort of legislation could be enacted to give OPM that authority, it certainly would help us as a user to adjudicate, to get all the information we need so we can make a proper adjudication.

---

[1] Subsequent to the hearing, Mr. Dalinsky supplied the following information for the record: "The DOE did participate in some of the panels established after the issuance of NSDD-84. However, I believe there has been little activity by these groups over the past year."

Additionally, in the Privacy Act realm, we have run up against instances where individuals have procured copies of their background investigations prior to our conducting an interview or prior to our going through our administrative due process, and we have instances where individuals have, even though the reports had been sanitized or depersonalized, identified the source of the testimony and threatened those individuals.

Consequently, we did work out a procedure, and this is in my written testimony, with the Office of Personnel Management and in conjunction with our Office of General Counsel, whereby in consideration of the fact that an investigation is not really complete until the final adjudication is made, we could reopen that investigation at any time.

Where we had cases that were going into a hearing, we worked with OPM to assure that the investigative reports, per se, would not be released or copies of the reports would not be released to the individual prior to the hearing.

Senator NUNN. The information would be made known but nothing that would give away the identity of the individual making the revelation.

Mr. DALINSKY. The reason why that was agreed to by everyone was because the intent of the Privacy Act is that you should not use information concerning an individual to make an adverse, arbitrary, or capricious adverse decision without them knowing why and how that decision was made.

In our administrative due process, we inform the individual of the derogatory information and advise them of their right to a hearing and at that hearing, it is up to us to produce witnesses and other sources of derogatory information, such as record testimony of derogatory information, so that the individual is aware of who is making the statements and is able to confront the witness to refute or rebut that information.

So essentially we cannot make an adverse determination without affording the individual those rights.

Senator NUNN. Thank you very much, Mr. Dalinsky. Senator Gore?

Senator GORE. Thank you, Mr. Chairman. I will be very brief. Mr. Dalinsky, we have heard that many agencies rarely revoke or deny security clearances. Is this true with the Department of Energy? Do you have any figures on how many you have revoked or denied?

Mr. DALINSKY. I do have some here. Since 1947, which is when the program began under the U.S. Atomic Energy Commission, one of our predecessor agencies, we denied or revoked approximately 7,700 clearances. In calendar year 1984, 72 clearances were denied or revoked.

Senator GORE. What recourse does DOE have with contractors who violate security requirements? Do you have the authority to fine them, and do you ever fine them?

Mr. DALINSKY. We don't have the authority to fine them. The way the procurement regulations and contractual agreements are stated, we do have the authority to close them down. What this means, and obviously this will pertain to a contractor involved in classified work for the Department, is if their implementation of the security requirements or lack of implementation of security requirements present a danger, in other words, an overt failure to protect classified information, we have the authority, in fact, to remove those classified interests. If those interests are closed down and removed then they can't work on the contract and, obviously, they can't be paid.

Senator GORE. Using another kind of metaphor, you have the ability to drop an atomic bomb on them but nothing short of that. You can't really do anything effectively to remedy the problem because there would be a natural reluctance to shut down the entire operation, wouldn't there?

Mr. DALINSKY. I think that would be the most drastic case.

Senator GORE. That is the only recourse you have under the law; is that correct?

Mr. DALINSKY. That's correct.

Senator GORE. Wouldn't it seem to make sense to have some recourse short of that to exert discipline and encourage contractors to comply with these requirements?

Mr. DALINSKY. I'm sure it would. There are, I think, other ways it could be influenced. I know in our GOCO's [government owned and contractors operated] facilities, and I am not a procurement expert so I don't know the technical aspect too well, so you will have to forgive me, but there is an award system where additional moneys can be awarded to contractors who perform in a superior manner. If their interpretation of DOE requirements are not up to standards, that is one area that could affect that award system.

I guess that could be considered, again, the second monetary type of——

Senator GORE [interposing]. Yes, but it never has been used that way.

Mr. DALINSKY. I don't know if it has been or not.

Senator GORE. Just as one member of this subcommittee, I will make the recommendation at the appropriate time when we begin considering a legislative proposal, if, indeed, it comes to that, that we include additional authorities below the extreme punishment of shutting the whole project down.

Let me ask you just a couple of brief questions on Mr. Veliotis. The subcommittee is going to have questions in writing for you on this matter, but he was given secret and top secret clearances from the Pentagon and "Q" access authorization from the Department of Energy.

Now, DIS told us they looked at the DOE "Q" clearance file on Mr. Veliotis during their security check. Can you confirm that DIS looked at your "Q" file on Mr. Veliotis?

Mr. DALINSKY. I cannot. If I recall correctly, in my review of the file, I do not recall any notation that the file was reviewed by any representative of the Department of Defense or Defense Investigative Service.

Senator GORE. Fine. Your "Q" clearance was granted when?

Mr. DALINSKY. In 1977. I believe it was October 1977.

Senator GORE. Was anybody at DOE aware of this unreported trip to the Soviet Union in 1973 while he was in charge of the Quincy Shipbuilding Division and oversaw the sensitive military nuclear propulsion information?

Mr. **Dalinsky**. He did list that. He listed the trip on his Department of Energy, or then Atomic Energy Commission security forms.

Senator **Gore**. At the time that he was granted "Q" clearance?

Mr. **Dalinsky**. Yes. His forms were submitted for processing. We require a listing of foreign travel, and he did have a trip listed on the back of the form. He had a rather extensive amount of travel. He did have a trip listed to the Soviet Union in 1973.

Senator **Gore**. DIS said it was unreported to them. I guess maybe if they had looked at your file, they would have found that.

Mr. **Dalinsky**. I assume so.

Senator **Gore**. Are you satisfied with the effectiveness of DOE's personnel security program affecting immigrant aliens and recently naturalized citizens?

Mr. **Dalinsky**. Sort of yes and no. That's an issue that we're reviewing at the moment.

Senator **Gore**. Elaborate on the "sort of no" part.

Mr. **Dalinsky**. The "sort of no" part that this would apply to, concerns not only to recently naturalized U.S. citizens, but also some American citizens as well born in the United States. One of the issues that came to light in our program a number of years ago was the problem of dual citizenship. We found, and I don't know why it didn't come to light before, we found there were many individuals out there who not only held U.S. passports but passports of other countries.

Most of the cases that came out were individuals who were naturalized U.S. citizens. Of course, when you become a U.S. citizen, naturalized, you take an oath wherein you vow loyalty to the United States. I don't know if there is a requirement that your passport be collected because, obviously, people are here under passports from other countries.

What we found is many individuals retain their passports and in some instances, in fact, continue to maintain their citizenship of another country.

While the United States doesn't recognize dual citizenship, there are many countries out there that do. I think somewhere between 50 and 60, according to the last figure I had from the State Department—Greece, Israel, United Kingdom, Taiwan, Republic of China—and we have many instances where people leave the United States under U.S. passport and we found who travel outside the United States on another country passport and then reenter back into the United States on a U.S. passport.

Obviously, to us that presents a problem of dual loyalty and now we ask on our questionnaire whether or not an individual has dual citizenship status. If the answer is yes, we interview them on that. Even if the answer is no, we do ask the investigative agencies to check as best they can. If they admit to dual citizenship status, we ask them to formally renounce citizenship in the other country before we will continue processing the case for "Q" clearance.

Senator **Gore**. Of course, Mr. Veliotis had triple citizenship.

Mr. **Dalinsky**. Greek, Canadian, and United States.

Senator **Gore**. In some respects, my impression is that DOE is the one of the better handled agencies in this regard. I would like to thank you for your testimony here and thank you, Mr. Chairman.

Senator **Nunn**. Thank you, Senator Gore. Thank you very much for being with us his morning. We appreciate your help. If you have any other observations, we will keep the record open for them. We will have a few questions for the record, too.

Mr. **Dalinsky**. Thank you.

[Mr. Dalinsky's prepared statement and responses to written questions follow:]

STATEMENT OF
MR. A. BARRY DALINSKY
DEPUTY DIRECTOR
DIVISION OF SECURITY
OFFICE OF SAFEGUARDS AND SECURITY
DEFENSE PROGRAMS
DEPARTMENT OF ENERGY

* * * *

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS

APRIL 17, 1985

Department of Energy Employees and Security Clearances

Mr. Chairman and Members of the Subcommittee. I am pleased to be here today to discuss with you the personnel clearance program of the Department of Energy (DOE). Through its Personnel Clearance Branch, the Division of Security has responsibility for developing policy, standards, and procedures for the DOE personnel security program as well as carrying out the operational aspects of the Headquarters personnel clearance program. With me to assist in responding to your questions is Mr. John M. Miller, Chief, Personnel Clearance Branch, Division of Security. The Division of Security is a part of the Office of Safeguards and Security which reports to the Assistant Secretary for Defense Programs of the DOE.

As you know, it is the Defense Programs' area of the DOE that is responsible for designing, developing, testing, producing, and maintaining all of the United States' nuclear weapons in support of the Department of Defense (DOD). Most of our personnel security efforts are in direct support of DOE Defense Programs activities; however, ours is the single program for all Departmental personnel security activities since any clearance or access determination is for the purpose of protecting the common defense and security. The recent history of espionage and terrorist acts has heightened our concern over the protection of nuclear weapons, special nuclear materials, facilities, and classified information. We must be ever conscious of a wide range of threats in the form of espionage, unauthorized disclosure of classified information, or theft or diversion of nuclear materials; sabotage, particularly to one-of-a-kind facilities or operations; or the precipitation of a nuclear incident.

Originally, the Atomic Energy Act of 1946 required that the Atomic Energy Commission (AEC), a predecessor agency of the DOE, make a determination of eligibility for access to Restricted Data by any individual requiring such access authorization based upon reports of background investigation which were conducted for the AEC by the Federal Bureau of Investigation (FBI). Restricted Data is a special category of classified information concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy. In 1954, the Atomic Energy Act was amended to permit the AEC to use reports of background investigations conducted for the AEC by the U.S. Civil Service Commission as a basis for these Restricted Data access authorization determinations.

The 1977 Civil Service Reform Act abolished the former Civil Service Commission and established in its place the Office of Personnel Management (OPM). The Bureau of Personnel Investigations of the former Civil Service Commission remained with the OPM and it is that element of the OPM which continues to perform the majority of background investigations for the DOE as a preliminary step in the Department's access authorization determination process.

The FBI performs background investigations for the DOE only in those cases (approximately 10 percent) wherein the position to be occupied by an employee or a contractor employee is specified by the Department to be of a "high degree of importance or sensitivity" as defined in Section 145(f) of the Atomic Energy Act.

The DOE does not have investigative authority. The DOE does establish standards and specifications as to the scope and extent of investigations to be conducted by the OPM and the FBI. Investigations are performed on a reimbursable basis and are funded for a total of $34 million in FY 1985. Our program is the largest personnel security program outside of the DOD in terms of annual adjudications performed and actual numbers of individuals with active clearances. Most of our effort is directed toward DOE clearances for our contractor employees.

In addition, the Atomic Energy Act provides that reports of background investigations by other Federal agencies may be used in lieu of OPM reports provided the investigation meets a similar scope and a security clearance has been granted by the other agency based on the investigation. For your information, the DOE does not accept interview background type investigations in this regard since they do not meet the established DOE investigative scope.

National Agency Checks (NAC), in contrast to background investigations, consist of a check of fingerprint and investigative records of the FBI and the OPM. Other agency records checks as may be suggested by the applicant's prior history are also conducted during an NAC (i.e., military services, Immigration and Naturalization Service, Central Intelligence Agency, etc.).

Consistent with the Atomic Energy Act of 1954, as amended, the DOE personnel security system is such that all individuals associated with nuclear programs, including Government and contractor employees, who will require access to Top

Secret or Secret Restricted Data must be subject to a full field background investigation. Only if proposed Restricted Data access is to be limited to the Confidential Restricted Data level will the NAC type of inquiry suffice.

All background investigations are required to meet the common defense and security requirements of the Atomic Energy Act of 1954, as amended; the requirements of Director, Central Intelligence Directive (DCID)-1/14 for access to Sensitive Compartmented Information; or requirements of Executive Orders 10450 and 10865.

Operationally, access authorizations are granted by our Headquarters organization and by 10 DOE field offices located throughout the United States. This function is performed solely by DOE employees. For this and related personnel security duties we have less than 125 full and part-time DOE personnel involved in the personnel clearance function throughout the Department. This number includes both professional and clerical level staff.

Because of the material we were asked to address, one must carefully note that some information is given in terms of DOE employees only and some information is given in the much larger context of all personnel who possess DOE access authorizations. The DOE itself is a relatively small agency of about 16,800 employees, of whom 11,341 have been cleared.

A position is designated critical sensitive consistent with the Federal Personnel Manual (FPM) guidance. Determining position sensitivity designations is the responsibility of the field office managers and the heads of our Headquarters elements. There are approximately 5,300 critical sensitive positions in the DOE.

The DOE resolves personnel suitability for employment and personnel security for access to classified information through different elements of the organization. The specialized expertise and experience necessary to resolve the issues are different. We believe that personnel security decisions for access to classified information are directly linked to the national security and should not be subject to review by the U.S. Merit Systems Protection Board and the Federal Labor Relations Authority. Mixing suitability and security determinations may cloud the distinction between the two. For example, an individual may not be barred from some Federal jobs as unsuitable because he/she used illegal drugs off-the-job. However, such use of illegal drugs would definitely affect the adjudication of an individual's eligibility for a DOE security clearance.

Access

At the end of Fiscal Year 1984, the DOE had approximately 201,000 individuals (Federal, contractor, legislative, and judicial branch employees) cleared for access to classified information, special nuclear material, or DOE security areas. Because of the complexity of this data, I will outline it for the record.

Access to Restricted Data and National Security Information (NSI)

Secret and Top Secret Restricted Data and NSI	176,000
Confidential Restricted Data and Secret NSI	22,000

Access to NSI Only

Top Secret	500
Secret	2,500

DOE Federal Employees

Secret and Top Secret Restricted Data and NSI	10,300
Top Secret NSI	350
Confidential Restricted Data	500
Secret NSI	1,350
Total	12,500

The actual number of positions in the DOE that require access to classified information, special nuclear material, or DOE security areas will vary each year depending on programmatic requirements. The number of positions requiring access will correspond to the number of DOE employees having security clearances because, as access requirements change, supervisors and managers notify appropriate security officials and if access is no longer required by a particular individual the security clearance is terminated. Thus, there are no appreciable differences between the numbers of those cleared for access and those requiring access to classified information or facilities.

Specific criteria setting forth the responsibilities or considerations used in determining level of access is outlined in the DOE order on the Personnel Security

Program. Basically, the following considerations must exist to establish that a position be designated as "Q" sensitive which allows access to all classification levels of Restricted Data and NSI on a "need-to-know" basis.

1. Regular access to Top Secret Restricted Data, or
2. Regular access to Restricted Data involving broad policy or program direction, and this position may affect such policy direction in any of the following:
    a. research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production;
    b. production or stockpile of nuclear or thermonuclear weapons or special nuclear material;
    c. research, development, or production in the laser fusion or laser isotope programs; or
    d. naval nuclear propulsion program.

The following considerations are used to establish that a position be designated "Q" nonsensitive with access up to Secret Restricted Data and all levels of NSI on a "need-to-know" basis.

1. Access to Secret Restricted Data, or
2. Access to special nuclear material in Categories I and II, as defined in the attached DOE draft order 5631.2A.

The following considerations are used to establish whether a particular position requires a Top Secret access authorization:

1. Access to Top Secret NSI, or

2. Access to and development of war plans, or particulars of future, major or special operations of war, or critical or extremely important items of war.

And finally, a DOE "L" access authorization is granted to individuals who require access to Confidential Restricted Data and Secret NSI, while DOE Secret access authorization is granted to individuals who require access only to Secret NSI.

As a general rule, an individual must have a "Q" access authorization before being afforded access to Restricted Data. However, there are three exceptions to this rule. An "L" access authorization for access to Confidential Restricted Data is one exception. The other two exceptions relate to access by personnel of the DOD or its contractors upon certification of the appropriate access authorization and "need-to-know" and access by personnel of the National Aeronautics and Space Administration (NASA) or its contractors upon certification of the appropriate access authorization and "need-to-know." NASA's exception applies only for Restricted Data concerned with aeronautical and space activities.

We rarely grant access authorizations to foreign nationals or individuals who maintain dual citizenship. For access authorization to be granted, there must be a clear showing that the applicant has unique or very unusual talents or skills not possessed to a comparable degree by an available U.S. citizen and the position for which the individual is being considered must be one essential to the DOE's program. We currently have four foreign nationals with DOE access authorizations.

Background Investigations

I turn now to address the types of personnel investigations our agency utilizes for new employees or contractors by sensitivity of position.

For contractor employees, the level of access is the determining factor for what type of personnel investigation is to be conducted.

For DOE Federal employees, both position sensitivity and level of access required determine what type of personnel investigation is to be conducted. In terms of position sensitivity alone, the investigations utilized are those required by FPM Chapter 731. The DOE overlays those requirements with the following investigative requirements when access to classified information is also required:

Level of Access	Type of Investigation
Top Secret Restricted Data	Background Investigation (15 years)
Secret Restricted Data	Background Investigation (5 years)
Confidential Restricted Data	NAC
Top Secret NSI	Background Investigation (5 years)
Secret NSI	NAC

Our background investigations are conducted by either the OPM or the FBI. All NAC's are conducted by the OPM. The criteria for using the FBI for background investigations is found in the Atomic Energy Act of 1954, as amended, Section 145(f). Specifically, for any position designated as being "of a high degree of importance or sensitivity" the investigation shall be made by the FBI.

The number of background investigations conducted for the DOE by each agency for the past 4 Fiscal Years is:

Fiscal Year	FBI	OPM
1984	1,424	[illegible],603
1983	1,270	[illegible],067
1982	1,594	13,807
1981	1,443	15,023

In addition, the OPM conducts approximately 8,000 NAC's per year for our security program.

The average investigative times for background investigations is now about 109 days for the FBI and about 217 days for the OPM. Since the OPM does over 90 percent of our background investigations, its timeliness has the greatest impact on the DOE.

The current investigative time of over 200 days far exceeds the optimum investigation time of 60 days. As recently as early 1983, the OPM did provide excellent investigative times, but the rapidly growing caseload has exceeded the OPM's investigative resources. Short of reducing the scope of the investigation or the reporting format, there is little that the DOE can do to reduce investigative times. The current investigative time, plus our own internal processing procedures, results in many contractor employees having to wait 8 or 9 months before they can start working on the classified project that they were originally hired to perform. Such timeframes have resulted in lost productivity and, in some cases, may have resulted in the loss of highly qualified applicants, but there has been no degradation of the national security. Recent initiatives taken by the OPM to provide substantially greater investigative resources hold promise for restoring acceptable investigative times by late 1985.

We are satisfied with the scope of the investigations since the Atomic Energy Act of 1954, as amended, Section 145(g) establishes that the scope of investigations conducted for access to Restricted Data will be established by the DOE. As for quality, both the FBI and the OPM have continually provided us with a full, complete record of an individual's background which can only be classified as a product of the highest quality available given the many legal restraints which are placed upon the investigative agencies.

Critical sensitive positions are not normally filled prior to completion of the background investigation. However, when the services of a selectee are needed to meet a critical need and are required in the national interest as provided by section 3(b) of Executive Order 10450 and the FPM, a waiver of the preappointment investigative requirement may be made. In such emergency situations, a request is submitted by the employing organization with certification of the first tier organization head. Reviews are made by the Office of Safeguards and Security and the Director of Administration, with approval by the Secretary, DOE. This is done only when checks indicate that the possibility of derogatory information being developed is remote and meaningful work can be accomplished without access to classified information. If the individual is already a DOE employee when appointed to a critical sensitive position, the employee is precluded from access to classified material beyond that for which access has been authorized. For calendar year 1984, a total of 44 requests were considered.

With respect to suitability for current DOE employees, without regard to security, the Office of Personnel within DOE Headquarters is responsible for adjudicating information contained in the investigative reports that may impact suitability for Federal employment. Primary staff review is conducted by the Employee/Labor

Relations staff personnel and the final determination is made by the Director, Headquarters Personnel Operations Division. Their procedures involve consideration of the criteria for suitability contained in Chapter 731, titled Suitability, of the FPM, and clarifying OPM guidance along with case law generated by Merit System Protection Board (MSPB) decisions. Reported information is analyzed against the position requirements. When appropriate, input on the employee's conduct and performance is obtained from the employee's supervisor. A review is made of the employee's Official Personnel Folder and other relevant employment documents.

In cases involving a DOE security clearance, adjudication normally begins with a review of the investigative reports and all other pertinent paperwork to determine that the investigation is complete, to note discrepancies in information, and to note all information of a derogatory nature. Cases where the investigation is complete and no derogatory information is reported are appropriately documented and access is granted. If there is derogatory information, it is evaluated along with all other information, both favorable and unfavorable. If additional information is required, one may consider additional investigation, an informal interview, or psychiatric evaluation, if applicable. Most cases involving this further action will result in a subject interview. DOE-wide, perhaps 4,000 interviews are conducted annually to clarify or resolve information. These indepth subject interviews are particularly fruitful in either resolving the information sufficient to grant access or in developing critical information used in an administrative hearing.

For cases that cannot be resolved favorably through the procedures above, the next step is normally the administrative "due process" procedure outlined below.

For DOE employees involved in adjudicating an individual's eligibility for access, senior field office adjudicators normally train individuals on-the-job and this is supplemented by periodic DOE Headquarters training seminars in such areas of concern as interview techniques and administrative review procedures.

Since 1947, the DOE has processed 1,285,000 individual cases for access. Approximately 14,000 cases have gone through administrative review of which 6,300 individuals were granted or continued access and 7,700 individuals were denied or revoked access, or discontinued processing.

The tabular material that follows indicates the number of clearance denials and revocations that were made by the Assistant Secretary for Defense Programs for the last 3 calendar years.

	DENIAL	REVOCATION
CY 1984	42	30
CY 1983	21	16
CY 1982	24	17

The administrative "due process" procedure used by the DOE for applicants (Federal and contractor employees) and individuals granted access (Federal and contractor employees) is outlined in 10 Code of Federal Regulations Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material."

In brief this procedure includes:

1. Possible suspension of access already granted to an individual, pending the outcome of the administrative procedures;
2. A notification letter setting forth detailed information about the questions concerning eligibility and procedural rights to an impartial hearing;
3. The right to appear before a Hearing Officer and present evidence in his/her own behalf, to confront and cross examine witnesses, and be represented by counsel or representatives;
4. The right to appeal a Hearing Officer's adverse finding to three independent Personnel Security Review Examiners; and
5. Subsequent possibility for reconsideration where there is a bonafide offer of employment and new evidence of reformation or rehabilitation.

We fully support and have continued to support the.DOE implementation of the provisions of the Privacy Act. However, we believe that individuals who provide the OPM and FBI with information in the conduct of a background investigation for national security purposes must also be protected. About 3 years ago, we noted that a trend was developing wherein some DOE clearance applicants who had been advised by the DOE that their case would be processed under DOE administrative review procedures were obtaining a copy of their background investigation under the provisions of the Privacy Act prior to the scheduled DOE Personnel Security

Hearing. After obtaining a copy of their background investigation, some applicants then contacted the sources of the derogatory information and threatened these sources if they testified against the applicant at a DOE Personnel Security Hearing. As a result of these threats, the sources then contacted the investigative agency and altered their original testimony to delete the derogatory information or refused to testify at the DOE hearing. In response to these incidents, we established a procedure with the OPM, consistent with the Privacy Act, whereby a copy of a background investigation would not be released to a DOE clearance applicant who was being processed under DOE administrative procedures until such time as the DOE hearing was concluded. By implementing this procedure, we attempted to insure that sources of derogatory information would not be confronted or threatened by the clearance applicant prior to the conduct of the DOE hearing while continuing to assure that the DOE clearance applicant did receive a copy of his/her background investigation in accordance with the provisions of the Privacy Act. Pursuant to written instructions on security hearings, a clearance applicant is furnished the adverse information which will be introduced at the hearing in order that he/she can prepare to rebut it. Again, our procedures were implemented not to prevent an individual from having access to his/her records, but to insure that the national security interest and the well-being of sources of information are protected as well as the interests of the DOE clearance applicant.

To institute the administrative review procedures, the individual must be provided a notification letter, approved by DOE Legal Counsel, that sets forth the information which creates the substantial doubt regarding the individual's eligibility. Such information must be as comprehensive and detailed as the national security permits. The administrative review procedures require that the subject or his/her representative be provided with a witness list and copies of all record information (public documents) which are to be introduced by the DOE no less than 10 days prior to the hearing. Additionally, if the subject requires witnesses for his/her case, the DOE will subpoena witnesses as required. The DOE adjudicates cases on the basis of witness testimony presented at the hearing where the subject may confront and cross-examine such witnesses, rather than upon reports of investigation. The final decision in a security case is made by the Assistant Secretary for Defense Programs on the basis of the hearing record only. Our confidence in these procedures is such that we can accept that final decision with complete satisfaction.

One substantial concern to us is the inability of the OPM to obtain record information (arrest/employment) from many states as a result of State privacy act laws which have very fine definitions as to what is a "law enforcement" agency. This problem is further compounded because the National Crime Index Center has refused to issue OPM a user number for access to criminal history information.

The DOE Reinvestigation Program is designed to review the continued eligibility for access authorization of individuals in our classified programs. We believe this program is important because individuals and circumstances change over time.

Through reinvestigations we discover situations that preclude continued access. In general, reinvestigation applies to all individuals possessing DOE security clearances except other Government agency personnel and DOE contractor construction personnel. In our current updating of policy, individuals holding DOE access authorization will be reevaluated every 5 years on the basis of either a full field investigation, NAC with Credit, or file and fingerprint check and review of the Personnel Security Questionnaire. For example, those with clearances requiring full field investigations have full field investigations again at the 5 and 20-year intervals and NAC's with Credit at 10 and 15-year intervals as well as at 25 years and every 5 years thereafter. Full field investigations are performed by the original investigating agency and the NAC by the OPM. Reinvestigations cost the same as original investigations, however, we do schedule our OPM reinvestigations for 120 days rather than the normal 75 days since the cost is about 10 percent less. In addition, we often flag cases for reinvestigations of satisfactorily adjudicated situations which had previous derogatory information; for example, prior drug and alcohol use and financial problems. We also believe our Personnel Security Questionnaire is a particularly effective tool in identifying information requiring further investigation. For FY 1984, we requested about 2,200 full field reinvestigations.

Criteria and standards for the adjudication of periodic reinvestigations are the same as those utilized for initial adjudication. Since reinvestigations involve individuals with continuing access, it may be necessary to suspend authorization in some instances pending the outcome of administrative review to resolve developed derogatory information. For FY 1984, 30 revocations resulted from reinvestigations.

Criticism alleging waste or suggesting inadequate control of contractors sometimes surfaces in the security area. The DOE, through its several field offices, exercises tight control on the need for and level of clearances granted. Where current appropriate investigations and clearances by other agencies exist, we take advantage of those to save further investigative cost. However, we do our own adjudication of these cases. We have improved our Personnel Security Questionnaire, completed by all clearance applicants and employees, to reflect the types of information needed for investigation and adjudication of cases. To minimize underutilization of contractor employees due to lack of clearance, DOE acquisition regulations provide:

> "When an applicant is being hired specifically for a position which shall require a DOE security clearance, the applicant shall not be placed in that position prior to the security clearance being granted by the DOE unless an exception has been obtained from the Head of the Contracting activity or designee."

To reduce security issues that should have been avoided through employment considerations, the DOE requires that all Government-owned-contractor-operated (GOCO) facility contractors perform specific suitability preemployment checks on potential employees.

In the area of facility security, the DOE has a survey program which provides for Government oversight over a contractor's performance vis-a-vis DOE security requirements. Specific written assurances from the contractor are required prior to their receipt of any classified information. Typically, each contractor with the DOE agrees under the terms of their contract to meet all DOE security regulations, requirements, and policies.

The DOE has a total of 569 cleared facilities ranging from those engaged in major activities of the Department, down to those in which Restricted Data is simply originated, received, or stored. Of these, approximately 60 are class A facilities. Class A facilities are either engaged in administrative activities essential to the overall DOE program, engaged in various weapons activities, engaged in major uranium enrichment activities, involved with Top Secret documents over an extended period, or possessors of certain specified quantities (Category I) of special nuclear material.

Classified matter or special nuclear material is not permitted on DOE premises until the DOE has granted facility approval based upon a determination that satisfactory security safeguards can be afforded the DOE interests. Normally such a determination is based upon an initial onsite security survey wherein a physical security specialist reviews the facility and determines what measures must be taken to meet DOE standards and requirements necessary for approval. Onsite security surveys are conducted initially and periodically, at intervals determined by the class of the facility, to assure that DOE safeguards and security policies and procedures are implemented and that continuously satisfactory security is maintained for the DOE interests.

It is the contractor's responsibility to ensure that all security interests under its cognizance, including Restricted Data, are afforded appropriate safeguards. This includes measures to control access to classified information to properly cleared individuals who have a "need-to-know." It is the DOE's responsibility to provide onsite inspection and oversight over the contractor to ensure this compliance.

Followup by the cognizant DOE security office is required by DOE orders. Operations office managers have the authority to remove facility approval from contractors in situations where security is inadequate. Such decisions are made in coordination with the sponsoring DOE program organization and with the Headquarters Office of Safeguards and Security. When classified or special nuclear materials operations cease and these materials are removed, facility approval is terminated.

As a final item, I would like to mention briefly that one of the recommendations of the President's Private Sector Survey on Cost Control (Grace Commission) suggested that the use of the Defense Investigative Service (DIS) to conduct security investigations for the DOE would save substantial money. DOE consideration of the Grace Commission's recommendation established several points:

- The DOE is required by law (Atomic Energy Act of 1954, as amended, Section 145) to use the FBI or the OPM for investigations involving Restricted Data access. Legislative change would be required to permit the DOE's use of the DIS to conduct investigations.
- As evidenced by a GAO Report to the Congress (GGD-81-105) dated September 15, 1981, the DOE had serious concern that the DIS could deliver a product of similar quality, effectiveness, or integrity as that provided by the FBI and the OPM.
- Projected cost savings might be offset were the DIS to provide investigative reports in the required format and covering the number of information sources now covered by the FBI and the OPM.

Uncertainty over the cost of and ability to provide background investigations of a scope determined by the DOE for its purposes led to contacts with those in charge of the DIS. Despite the DOE providing extensive information on the coverage and format desired, the DOE was unsuccessful in obtaining a response that would confirm that the product we needed could be provided, or an indication of what the cost might be. Our own observation is that the DIS does not obtain the neighborhood coverage we require, nor provide the full reporting format required.

The Atomic Energy Act of 1954, as amended, provides that the DOE (the Commission in the Act) shall establish the specifications for the scope and extent of investigations. The DOE has been quite successful in obtaining a product tailored to its needs with the current investigative sources. We believe the OPM's report stands out in its full reporting format which provides the DOE adjudicator with a good indication, both favorable and unfavorable, of the total individual. The quality and thoroughness of the contacts made during the investigation are revealed through the depth of inquiry and the candor of the sources. The DIS does not present evidence that it would provide other than its standard product, which would not be acceptable for our needs.

That concludes my formal statement. I am submitting a number of pertinent materials that you may wish to include in the record:

- o Draft DOE Order 5631.2A
- o Personnel Security Questionnaire forms
- o 10 Code of Federal Regulations 710
- o DOE Preemployment Check Regulations

We will be glad to answer any questions the committee may have.

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * *

A. BARRY DALINSKY
Deputy Director
Division of Security
Office of Safeguards and Security
DEPARTMENT OF ENERGY

Q. Would you comment on the effect of the Office of Personnel Management's (OPM) delays on Department of Energy's efficiency and effectiveness.

Lengthy OPM investigative times adversely affect sensitive and classified Department of Energy programs as potential contractor employees must currently wait an average of 8 months for a DOE clearance before they may work on DOE classified projects. In some instances, the result is lost productivity and, we believe, the loss of fully qualified candidates. Our concern about lengthy investigative times has been conveyed to OPM and we believe the actions OPM is initiating will reduce their investigative times to an acceptable level in the near future.

Q. Is there a problem with inconsistent personnel security investigations? Do you accept DIS's? If not, why not?

Personnel security investigations conducted by Government agencies are not the same with regard to scope, coverage, and reporting format, primarily due to the fact that most agencies structure the investigative requirements to fit a stated or perceived need or objective. We believe that an agreed to investigative scope, coverage, and reporting format would make it easier for adjudicators in all agencies to adequately evaluate an individual's eligibility for a clearance.

The DOE does utilize investigative reports from the DIS as a basis for adjudicating a DOE clearance applicant when the report meets the scope and coverage requirements of the DOE and when we can confirm that the individual was granted a clearance based upon such investigative reports. This action is taken in accordance with Section 145.c. of the Atomic Energy Act of 1954, as amended. While we believe that it is important to have some consistency in investigative scope, coverage, and reporting format, we also believe that it would be even more important to assure consistency in the adjudicative standards of the various Government agencies.

Q. Why is DOE more "successful" in adjudicating these derogatories than other agencies?

We believe a number of factors have contributed to our success in this area: strict procedural guidelines, a workable "due process" system, consistency in the application of our clearance criteria, and strict adherence to our established system.

Q. What is the single most serious problem with current personnel security system of the Government?

In our opinion, the single most serious problem in Government personnel security programs is the inability of some agencies charged with conducting background investigations, such as DIS and OPM, to adequately procure information with which an adjudicator can assess the potential risk to the national security in granting an individual a clearance. The following problems run a very close second: inconsistency of clearance criteria and its application, adequate staffing for investigations and adjudications, lack of a centralized index of clearance records and information, and lack of adequate training for adjudicators.

Q. Do you have any recommendations for Privacy Act?

We fully support the intent of the Privacy Act of 1974, but we believe some consideration should be made to enacting provisions that offer better protection to sources who provide information to investigators. However, we believe that such a change should only be enacted if assurances can be provided to the clearance applicant that "due process" procedures will be offered so that the applicant has the opportunity to refute/rebut any derogatory information that is used by the Government in the clearance determination process. This should be done to protect the clearance applicant against arbitrary or capricious action that could affect his/her eligibility or continued eligibility for a clearance.

Q. Does the Merit Systems Protection Board (MSBP) review your decisions? If not, why not? Should they?

While the MSPB has never reviewed our clearance decisions, it has reviewed decisions of other agencies where a Federal employee was discharged after losing his security clearance. We do not believe the MSPB should exercise such authority and have joined other agencies such as the U.S. OPM and other agencies in an amicus brief challenging their authority. We believe that matters involving national security should remain outside the purview of the MSPB.

Q. In your statement you refer to "no degradation of the national security." What is DOE's position on granting waivers? How do you ensure that waivers are not needlessly granted?

It is DOE policy that waivers of preappointment full field investigations for employees will be granted only under the most exceptional circumstances and when such action is clearly within the national interest. A waiver of the preappointment full field investigation for an employee applies only to that employee's occupying a critical sensitive position and such a waiver does not permit or authorize access to classified information. On rare occasions, Interim Access Authorizations are granted to DOE clearance applicants in accordance with strict policy guidelines. A preappointment full field investigation waiver and an Interim Access Authorization are considered temporary measures pending completion of a full field investigation and must be approved by the Secretary of Energy or the DOE Assistant Secretary for Defense Programs only after a security review of the individual's clearance forms and the conduct of indices checks. We ensure that such actions are not taken needlessly by: maintaining approval authority at the highest management levels of the Department, requiring adequate justifications for such request, and by requiring a positive security recommendation before such requests are further processed through the management chain.

Q. Would such a procedure be effective in other agencies?

We believe such a procedure would be effective in other agencies.

Q. What's the problem with DIS's IBI's?

Interview background investigations, or IBI's, as conducted by DIS do not meet the investigative scope and coverage requirements of the DOE.

Q. In the OPM investigations do you get copies of what the individuals say or merely summaries? Which is preferable? How does this compare with DIS investigations?

The OPM reporting format includes a full reporting of an individual's comments. We believe that this is an excellent format and product that provides our adjudicators with adequate indicators, both favorable and unfavorable, of the individual's character, habits, and associations. We prefer an indication of a source's full testimony rather than a summary of his/her statements.

Normally, the DIS background investigations provide a summary of a source's statement.

Q. What are DOE's procedures for adjudication? Are they clear and specific enough? Could these be used by other agencies?

For DOE access authorizations, adjudication normally begins with a review of the investigative reports and all other pertinent paperwork to determine that the investigation is complete, to note any discrepancies in information, and to note all information of a derogatory nature. Cases where the investigation is complete and no derogatory information is reported are appropriately documented and a DOE clearance is granted. If there is derogatory information, it is evaluated along with other information, both favorable and unfavorable. If additional information is required, we consider additional investigation, an informal interview, or psychiatric evaluation, if applicable. Most cases involving this further action will result in a subject interview that is particularly effective in either resolving the information or eliciting further information that would be of use in the conduct of an administrative hearing. When derogatory information cannot be resolved favorably through these methods, the next step normally is to convene an administrative hearing. We believe our procedures are clear, specific, and designed to address issues of security concern in a well documented manner. Many other agenices probably approach the adjudication process in a similar manner or could do so.

Q. Do you feel there should be consistency throughout the Government in the application of criteria? What is the problem now?

There must be consistency throughout the Government in the application of clearance criteria in order for personnel security programs to maintain an acceptable level of integrity in protecting the national security and the rights of the individual. The problem now is that, in some instances, other objectives or needs of an agency are factored into clearance adjudications that cause a final determination that may not be in the best interest of the national security or necessarily fair to the individual involved.

Q. We notice that you separate security from suitability in the Department of Energy. Why? Should this be applied to other agencies?

In the DOE, security and suitability determinations are separated as adjudications in each area require separate expertise and experience as to how the developed derogatory information may affect the national security or an individual's capability to adequately perform his/her duties. The DOE does have programs and activities of an unclassified and nonsensitive nature wherein an individual might be employed even though derogatory information exists which has precluded the granting of a DOE clearance. Our approach might be utilized in agencies similar to the DOE where their is a separation between classified and unclassified programs, but our approach probably could not be used in an agency where an individual must have a clearance in order to perform his/her duties; for example, as in an intelligence mission oriented agency.

Q. Your security adjudication standards have been in existence since 1947. Do you find it difficult to work with these due process procedures?

We believe our procedures provide us with an effective method of determining an individual's eligibility or continued eligibility for a DOE access authorization. Of course, while our procedures have been in effect since 1947, a number of changes have occurred in the procedures over the last 38 years. Our procedures are structured to permit this flexibility and to respond to changes that occur in the mores of society and the threats to the national security. As our clearance criteria and administrative due process procedures are a part of the Code of Federal Regulations, all changes thereto are published in advance for public comment. Our procedures are time consuming and incur a certain expenditure of Departmental manpower and funds. However, we believe that the benefits to the national security of such procedures far outweigh these difficulties.

Q. Two of the criticisms of due process procedure like DOE's is that it is so time consuming and expensive. How long does it take? Can you revoke or deny in the interim?

Within the time constraint's suggested in our procedures (10 CFR Part 710), the due process procedure should take no more than 1 year. For DOE clearance applicants, the final clearance determination is not made until the process is complete; therefore, no access to classified information or special nuclear material is provided unless there is a final favorable determination. For individual's who possess a DOE clearance, a decision may be made to suspend their clearance before the due process procedure begins. Suspensions are enacted prior to the administrative review process.

Q. Could these be applied across the Government?

We believe a similar approach can be applied to most Government agencies.

Q. How important are investigations? What is the policy of DOE?

Investigations are extremely important in providing independently derived information concerning the individual and an assessment of the individual's characteristics in terms of whether that individual is or is not an acceptable security risk. It is DOE policy to have investigations completed prior to an adjudication of an individual's eligibility for a clearance, to request such investigations according to the level of access required, and to independently evaluate and adjudicate the information provided in such investigations.

Q. On page 15 you refer to OPM having a problem in obtaining information because of not having an NCIC number. What do you mean by that?

OPM, in some states, is not provided access to criminal records as they are not designated as a law enforcement agency. If OPM had an NCIC identification number, their investigators would be provided access to state criminal records and thus could, in turn, provide this information to DOE. Without such information, the DOE must adjudicate certain criminal record information based solely on statements provided by the clearance applicant.

Q. In a 1982 ad hoc report to the Secretary of Energy were similar recommendations made? What was the end result of that recommendation?

Yes, a similar recommendation was made to the Secretary of Energy as a result of the findings of the ad hoc committee. The Assistant Secretary for Defense Programs sent a letter to the Department of Justice supporting the OPM's request for an NCIC number, but to the best of our knoweldge, no action on this issue was taken.

Q. It is our understanding that there has been a recommendation made by the Board of Governors of NCIC that henceforth only the first arrest will be reported to NCIC, all records of subsequent arrests will be maintained by the states. Will this negatively impact on DOE's Security Office for secret clearances?

If such an action is adopted, there could be negative impacts on all levels of DOE clearances if criminal arrest information is not made easily available for investigators. Additionally, we believe such an action would lessen the reliability/integrity factor of the NCIC program. Any changes to the NCIC program should be implemented carefully to assure timely and accurate reporting of all criminal arrest information.

Q. In examining personnel security programs in the Government, the subcommittee is studying the procedures followed when immigrant aliens and recently naturalized citizens apply for "Q" access authorizations and other clearances from the Energy Department and other agencies. To demonstrate these procedures at work, the subcommittee has looked at the manner in which P. T. Veliotis, a citizen of Greece and Canada and later the United States, received secret and top secret clearances from the Pentagon and a "Q" access authorization from the Energy Department.

The 1977 inquiry by the FBI into Veliotis' background turned up questions about the accuracy of certain of his assertions about his own past made in the Energy Department personnel security questionnaire.

--Was the FBI able to verify any of Veliotis' claims about his military service in the Greek Navy? Or about his reported attendance at the Greek Naval Academy?

> The FBI report provided to the DOE contained information provided by another agency that reflected that Veliotis had attended the Greek Royal Naval Academy from 1944 to 1947, but that he did not graduate from the Academy. This information was provided as a result of neighborhood inquiries in Greece. The FBI report also reflects that it was not feasible to verify Veliotis' claimed military service in the Greek Royal Navy.

--Did the FBI find that Veliotis had been convicted of and given a 45-day prison sentence for money order violations in 1954 in Piaeus, Greece? Did this finding raise questions about Veliotis that he had emigrated to Canada in 1953? Did this finding raise questions about Veliotis' assertion that he had never been convicted for a crime?

> The FBI report on Veliotis provided to the DOE reflected that Greek criminal records disclosed that he had received a sentence of 45 days imprisonment, in accordance with Decision #10 of June 7, 1954, of the Piraeus Court of Misdemeanors for the issuance of "uncovered money orders." While this fact was noted in Veliotis' DOE Personnel Security File, as well as the fact that this reported criminal conviction in 1954 was not listed by Veliotis on his Personnel Security Questionnaire, there is no indication in the file as to how this matter was adjudicated in the DOE, nor is there an indication that the criminal conviction date was questioned by DOE security officials in relation to the 1953 date Veliotis listed on his Personnel Security Questionnaire as having emigrated to Canada.

--Did Veliotis make an unreported trip to Russia in 1973 when he was in charge of the Quincy Shipbuilding Division and oversaw sensitive military and nuclear propulsion information? Was this in violation of the Defense Department's Industrial Security Manual?

> Veliotis reported on his Personnel Security Questionnaire that he did travel to Russia in 1973. Apparently, according to information now at our disposal, if this trip was not reported to the Department of Defense, such action was in violation of the reporting requirements then listed in the Defense Department's Industrial Security Manual.

In the face of these inconsistencies and unanswered questions, Energy Department gave Veliotis a "Q" access authorization, a clearance similar to what is a DOD top secret clearance.

--Should such a clearance have been given without further inquiry?

> Further inquiries into these inconsistencies should have been conducted by DOE security officials.

--Would you characterize the Veliotis personnel security procedures as being adequate or inadequate?

> We would characterize the actions taken in this case as inadequate and not in conformity with the required personnel security procedures at this time.

--Are there safeguards built into the system today that would require further inquiry should similar doubts be raised about the accuracy of an applicant's assertions about himself?

> Additional system safeguards in place at this time include periodic reviews of the DOE field office implementation of the Personnel Security Program by DOE Headquarters security staff and independent reviews of the entire program by the DOE Inspection and Evaluation Division and the Office of Personnel Management. Also, personnel security adjudicators and interviewers are now formally trained and the personnel security guidance has recently been updated. The DOE Personnel Security Program enjoys excellent support from all levels of DOE management and there is strict adherence to the requirements for approving foreign nationals for processing for a DOE access authorization, as well as strict adherence to the requirements for adjudicating investigative reports on foreign nationals once the processing has been approved.

Q. Veliotis enjoyed citizenship in three countries--Greece, Canada, and the United States. Does the question of dual citizenship cause you any concern from a personnel security point of view? Do you have any suggested remedies?

> Individuals being processed for a DOE access authorization who possess dual citizenship status present a serious security problem. The types of security concerns that must be addressed in such cases relate to possible split loyalties on the part of the individual, family or financial ties to the other country, and acceptance by the individual that he/she can be protected

under the laws of the other country. If the individual is a naturalized U.S. citizen, a question is raised concerning the individual's intended adherence to the oath of citizenship that he/she took upon becoming a U.S. citizen. In such cases, the DOE procedures require the individual to be interviewed prior to the processing of their clearance request in order to obtain additional data and to inform the individual that the DOE will not process the request for an access authorization for the individual as a U.S. citizen unless the individual formally renounces their other country citizenship. Such formal renunciation requires the individual to contact the other country embassy or consulate in the United States in writing to inform them of their intention and to provide to the officials of that country any valid passport that the country may have issued to the individual. Not all countries that recognize dual citizenship permit an individual to renounce their citizenship, and many that do permit such renunciation may not inform the individual that such a renunciation has been formally accepted. However, the DOE does accept the individual's actions as a clear demonstration of their intent and then processes the individual for a DOE access authorization. If the individual refuses to formally renounce their other country citizenship, then he/she is processed for a DOE access authorization in accordance with the DOE procedures for processing a foreign national.

Q. Are you satisfied with the effectiveness of the Energy Department's personnel security program affecting immigrant aliens and recently naturalized citizens? If not, what would you do to change the system if you could?

We believe that the DOE's personnel clearance policies and procedures affecting the processing of naturalized U.S. citizens for a DOE access authorization are effective. However, we also believe that these policies and procedures should be revisited in light of possible changing threats presented by hostile intelligence services. We are currently reviewing the feasibility of revising our personnel security policies and procedures to require a minimal time period of U.S. citizenship and residency in the United States for naturalized citizens before the DOE will process such individuals for an access authorization.

Q. What was done with the information indicating that Veliotis had made a trip to Russia in 1973?

Although the information was noted, no effort was made to question Veliotis about the trip as security officials did not interview him concerning any information returned in his background investigation or concerning discrepancies noted in his security forms.

Q. Was the Energy Department aware that the Industrial Security Manual (paragraph 6B(1)) required that trips to Communist countries by cleared personnel, including directors, had to be reported to DISCO?

We cannot state with authority whether security officials of ERDA were aware of this requirement as the officials involved in the clearance processing of this case are no longer employed by the Department.

Q. Was an effort made to find out if Veliotis' trip to Russia had been reported to DISCO according to established procedures?

Our review of the DOE Veliotis Personnel Security File reflects no notation that such an effort was made by security officials.

Q. Did Veliotis report the Russian trip to DISCO? Did General Dynamics report it?

There is no indication in the DOE file on Veliotis that such information was reported. We have not been afforded access to the DIS file on Veliotis but assume that the DIS file would contain such information if it had been reported.

Q. If the report was not made, was that sufficient grounds to deny the "Q" access authorization request?

The only way it could be determined whether such information would have been sufficient grounds for denying a "Q" access authorization would have been to process the case under DOE administrative review procedures in accordance with the provisions of 10 CFR Part 710. The answer to our questions, however, might have been resolved in the course of a personnel security interview had one been conducted by security officials.

Q. What is the significance of the handwritten notation "not listed."?

The notation appears to indicate that the material contained in the FBI investigative report was not listed by Veliotis on his Personnel Security Questionnaire.

Q. In adjudicating Veliotis' request for a "Q" access designation, did the Energy Department note the apparent conflict in dates? That is, Veliotis said in his Atomic Energy Commission (AEC) Personnel Security Questionnaire that he began working for Davie Shipbuilding in 1953 in Quebec. He used the 1953 date whenever asked for the year he emigrated to Canada. This would conflict with the reported June 1954 conviction in Piraeus, would it not?

Our review of the Veliotis file reflects that the discrepancy in dates was not noted, per se, although the reported arrest information from Greece was noted.

Q. Is a money order fraud conviction grounds for the denial of a "Q" clearance?

Depending upon the circumstances associated with the alleged incident, such a conviction might or might not be grounds for a denial of a DOE access authorization. Such a determination could only have been made after Veliotis was afforded administrative due process procedures under 10 CFR Part 710.

Q. In the same AEC questionnaire, there is another question in dates. Veliotis wrote that he obtained a "B.A." degree from St. Paul's College in Piraeus in 1942. According to his stated date of birth, August 11, 1926, Veliotis would have been 16 in 1942. Did this assertion that he had earned a B.A. degree at 16 raise any questions about the validity of his questionnaire?

> There is no indication in Veliotis' DOE Personnel Security File that this fact was noted or questioned.

Q. AEC personnel security requirements call for special procedures regarding clearances for aliens. These are set down in AEC Appendix 2301, Personnel Security Program. Were these special procedures followed in the Veliotis investigation/adjudication? If not, why not?

> Not all of the special procedures were followed in the Veliotis case. In particular, the requirement for a security interview was not followed. Had that requirement been followed, a number of questions might have been answered. We cannot speculate as to why the security requirements were not followed as the individuals involved with the processing of the case are no longer employed at the DOE.

Q. Did DOE have access to the DIS inquiry done in 1973-74 preparatory to his obtaining a secret clearance?

> Information concerning the DIS inquiry and record of clearance grant was reported by the FBI in its investigative report. A copy of the DIS report was not provided to the DOE security officials.

Q. Did DOE formally refer the results of the FBI investigation regarding the reported Piraeus conviction to DIS?

> There is no indication in the DOE Veliotis file that such information was reported to DIS. As this was an ERDA clearance action, and under our procedures at that time, the information would only have been reported if an action were taken by the DOE to process Veliotis' case under administrative review procedures.

Q. If not, why not? Wasn't this information properly the domain of DIS as well as Energy?

> Under ERDA procedures at that time, and under DOE procedures currently, such information is not normally provided to another interested agency as a routine procedure unless action is taken upon that information to process an individual's case under administrative review procedures. Our security files are always available to another Federal agency for review purposes based upon a legitimate request, and the DIS could have, at any time, received a copy of the report direclty from the FBI as the investigative report is their property and not the property of the DOE.

Q. In giving Veliotis a top secret clearance in 1980 DISCO relied on the "Q" access authorization as its justification for waiving the requirement for a background inquiry. What communication went on between the Energy Department and DISCO or DIS with regard to that reciprocal clearance?

There is no indication in the DOE Veliotis Personnel Security File that the DIS or DISCO made such inquiries in 1980. Of course, such an inquiry could have been made but not noted in the security file.

Senator NUNN. Our next witness is Mr. Lawrence J. Howe who is vice president, corporate security, Science Applications International Corp., La Jolla, CA. Mr. Howe, we appreciate you being here. We also have with us Mr. Eli Flyer, consultant, manpower research center, Department of Administrative Sciences, Naval Postgraduate School, Monterey, CA. Both of you hold up your right hand. We swear all witnesses.

Do you swear the testimony you will give before this subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. HOWE. I do.

Mr. FLYER. I do.

Senator NUNN. First let me thank both of you for your splendid cooperation with the staff. You made a number of interesting recommendations, and I have read your testimony. I understand that both of you are prepared to summarize this morning, which will be helpful to us.

I suggest, Senator Gore, we proceed to have both statements and then ask questions, unless there is a clarification we need during the course of the statement, and then come back and ask both questions.

You both have a lot of experience in this area, and we are very grateful to you for your cooperation and your suggestions.

Mr. Howe, do you want to lead off?

TESTIMONY OF LAWRENCE J. HOWE, VICE PRESIDENT, CORPORATE SECURITY, SCIENCE APPLICATIONS INTERNATIONAL CORP., LA JOLLA, CA; AND ELI S. FLYER, CONSULTANT, MANPOWER RESEARCH CENTER, DEPARTMENT OF ADMINISTRATIVE SCIENCES, NAVAL POSTGRADUATE SCHOOL, MONTEREY, CA

Mr. HOWE. I have prepared a very brief summary of the portion of my testimony dealing with personnel security and summarizing several recommendations that I have for the subcommittee.

Senator NUNN. Without adding to your summary unnecessarily, give a little bit of background because not only are you key in the security industry, you also had governmental experience.

Mr. HOWE. Yes, sir. I have functioned as the vice president of corporate security for Science Applications International Corp. for the past 7 years. Prior to assuming those responsibilities, I functioned for 15 years in Government service with the Central Intelligence Agency as a staff security officer. During my tour of duty with the Central Intelligence Agency, I carried out personnel security assignments, including functioning as a polygraph examiner and my most recent assignment with CIA was as a regional industrial security officer.

Senator NUNN. Thank you very much.

Mr. HOWE. I would like to address the general area of personnel security. The size of our national defense effort requires that a staggering number of people be granted security clearances. It is small comfort so few of the people who have been cleared have betrayed this trust. Unfortunately, the amount of damage to our national security which can be caused by failure of a single individual is so great that no statistical probability of failure rate can ever be acceptable.

Security procedures, physical security barriers and all other external features of the security program, will not and cannot of themselves prevent espionage. In the final analysis, the trustworthiness and reliability of each individual granted access to classified information can be the only effective deterrent for the loss of our vital defense secrets.

It's the purpose of this testimony to raise the question of whether current government industrial security clearance practice can be more effective through consolidation, coupled with an increased emphasis on human reliability studies.

The premise of this position is that present personnel security procedures are decentralized at the risk of dilution and too much effort is expended on multiply clearing individuals that could be better spent reinvestigating.

A serious issue involves whether a centralized clearance adjudication for DOD special access clearances might not only be more cost effective, but enhance standards and consistency. Presently, much readjudication is carried out on special access program activities and sensitive compartmented information programs that might otherwise be avoided in the interest of having a more effective reinvestigative job done.

I would like to now summarize a comment on one of the underlying assumptions of the adjudicative process. A clearance adjudication is a decision based on the assumption that most of us use in making our own decisions about people. We generally believe that a person's past history is indicative of future behavior. While most of the time the assumption holds up, there are unfortunate exceptions.

Fundamentally, the issue is change. During change, the decision-making framework undergoes modification. The greater the changes which an individual undergoes and the greater the pressure to change quickly, the lower the validity of predictive assumptions based on past behavior.

The most important proposal which I can make to the subcommittee to enhance security clearance effectiveness is that more attention needs to be directed to human reliability studies. For example, the implications of stressful change made over a short time-frame need to be better understood. The reinvestigative process needs to be more pro-active rather than reactive. Effort needs to be focused on better early-warning signs.

As a suggestion, one potential resource for developing early-warning signs might be the adoption of an annual life event inventory profile. Contemporary mental health emphasis on stress management techniques utilize such an inventory to predict the probability of stress-induced health problems. These profiles exist in various forms and are based on an assignment of numerically weighted values to a series of events which people experience during their lifetimes.

What is significant about the insights gained from these studies is the cumulative effect of a series of events which, taken separately, would have relatively low stress values.

The interesting point is that an individual may be undergoing a significant amount of cumulative stress which is causing major changes in the decisionmaking framework, although only a minimal number of separate causative events are identifiable to outside observers.

I would like to now summarize four specific recommendations for the enhancement of the DOD contractor security clearance process.

First, strengthen the adjudication criteria determination role of the Defense Industrial Security Clearance Office. A human factors research activity should be attached to DISCO to coordinate and evaluate studies on human reliability. A much better understanding of the human decision-making process needs to be developed.

Much of the present adjudication standards take the form of a character flaw profile. If a clearance applicant displays any of the character flaws of a known traitor, such as a Burgess or McLean, the clearance is denied. The existing personnel security suitability standards concentrate on symptoms such as substance abuse, homosexuality, or excessive indebtedness without, in my opinion, an adequate understanding of the breakdown of the human decisionmaking process.

Why does one individual accept constraints and another take the risk of committing espionage? Conscience does not necessarily make cowards of us all. The profile of a traitor may not be significantly different from that of many sociopaths or felons. Loyalty to country has become so abstract that an act of treason is not necessarily different from any other serious crime.

What differentiates a traitor from a common thief may be little more than opportunity. The existing and extensive studies on criminal behavior need to be reviewed from the clearance point of view for insight. At present, there appears to be too little focus on this important resource.

Second, establish an annual review to determine the need for reinvestigation. The present clearance review process is structured to reinvestigate at 5-year intervals for those individuals approved at top secret level but not at lower levels. In practice, even this goal has not been adequately met because of insufficient investigative resources.

Once granted, secret clearances do not presently receive any further investigative action unless adverse information is developed which necessitates the reinvestigation. Given that clearance approvals, in my opinion, are not truly predictive of future events, aggressive reinvestigative efforts for all clearances is essential.

Each individual cleared under the Defense Industrial Security Program should be asked to submit a brief annual update form which would highlight significant changes which occurred during the past year. The survey could be supplemented with a modified form of a stressful event inventory, which I discussed a moment ago. These annual updates should be reviewed by the contractor security manager prior to submission to DISCO. Those statements reflecting questionable activity or a significant amount of stress-change factors could be highlighted for immediate DISCO action.

Based on these inputs, better focus could be given to reinvestigative efforts. The necessity to participate in an annual update would also reinforce personnel security awareness among cleared personnel.

Third, utilize interview techniques on all clearances, secret and above. The Defense Investigative Service has indicated an increase in developed significant information since the adoption of the interview augmented background investigation. This practice has been utilized to date in top secret clearance investigations. The activity should be expanded to include secret clearances and, in this regard, personnel security, investigative standards affecting sensitive compartmented information should be reviewed to reflect the positive results of the DIS approach.

Finally, consolidate all DOD Industrial Security Clearance adjudication at DISCO. DOD components involved in special access program or sensitive compartmented procurements presently carry out their own individual clearance adjudication. It is entirely appropriate, in my opinion, for procuring activities to make judgments concerning need to know. The duplication of clearance adjudication activity is another issue.

DISCO should have a special adjudication section established to handle the eligibility for clearance of all DOD contractor personnel requiring access through top secret sensitive compartmented information.

Director of Central Intelligence Directive 1/14 has established minimum standards for the entire national security community which must be met to grant clearance for access to top secret sensitive compartmented information.

The establishment of a centralized point for all DOD contractor adjudication, including SCI and SAP activities would ensure a higher level of consistency and afford a more informed basis for DOD review of clearance adjudication criteria.

I might make an aside, Mr. Chairman, some of the informal discussions I have had with procuring activities indicate that their greatest reluctance is their fear that they would not have the ability to make an input to prioritize cases which they now have with their own independent adjudication and investigative capabilities.

At present, much unnecessary separate re-adjudication is done on SCI and SAP activities. Significant savings and enhanced uniform standards could be achieved by a common centralized special access authority. Much of this adjudicative resource could be better utilized in support of the more aggressive re-investigative program.

It is my belief that the transfer of existing personnel slots from non-DISCO clearance adjudication to DISCO would, in all probability, be more than ample to handle the processing requirements without any overall negative Defense Department budget impact. Some economy of scale could be anticipated.

That concludes my statement.

Senator NUNN. One brief question. I have an urgent phone call I have to make so I am going to defer to Senator Gore to ask questions and then come back to Mr. Flyer. You indicated in here, and I didn't hear it in your oral summary, that we need to find a way not to have a disincentive for security on the part of the contractor. You are saying that cost-competitive contracts, which we all think we have to emphasize more and more from a tax savings point of view, have an incentive for the contractors to skimp on the security angle and you are saying that we need to find a way to remove that disincentive.

Mr. HOWE. Yes, Senator, that's correct. We certainly all support the emphasis on competitive procurement for the Government to get the best possible product at the most cost-efficient price. However, a negative fallout is that present Federal acquisition regulation procedures for competitive procurements recognize the contractor's costs spent on security in the overhead pool.

As a result, those contractors who spend less on security in effect have a competitive advantage under the present competitive procurement practice than the contractor who is conscientious and fully supports and funds an effective security program.

So there is, in effect, an unintended but effective disincentive.

Senator NUNN. And your suggestion is that we separate that portion out so it can be separately evaluated?

Mr. HOWE. Yes, sir. I think it is possible to look at the Federal acquisition regulations and for at least the contract award consideration, isolate those costs out for security and have them not part of the pool that is considered in the total cost package that is being evaluated.

Senator NUNN. Are those costs separable from a contractor point of view?

Mr. HOWE. Yes, sir; I believe they are.

Senator NUNN. Senator Gore, I yield to you and I will be back in a moment.

[At this point in the hearing, Senator Nunn withdrew from the hearing room.]

[Letter of authority follows:]

UNITED STATES SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, DC.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive session hearings without a quorum of two Members for the administration of oaths and taking testimony in connection with hearings on "U.S. Government Personnel Security Program." These hearings are to be held on April 16, 17 and 18, 1985.

BILL ROTH,
Chairman.
SAM NUNN,
Ranking Minority Member.

Senator GORE [presiding]. I would like to begin with one that is kind of theoretical, really, that results from the last witness. Would you agree that it is ridiculous to require more extensive background and security checks for people who do not have access to classified information than for people who do?

Mr. HOWE. Senator Gore, my understanding of the scoping criteria for investigations is that the more critical the access the individual is anticipated to have, the greater the extent of background information the adjudicator would like to have.

Senator GORE. Right.

Mr. HOWE. Ideally, in all cases you would like to have the maximum amount on every individual. But I think as we heard the numbers of clearances involved, the majority of the adjudicating authorities will settle for a lower level background information for a lower level of clearance.

Senator GORE. The reason for that is you have to establish priorities?

Mr. HOWE. Yes, sir.

Senator GORE. Taking this one step further, if you have a limited number of people assigned to conduct such background checks, and a limited amount of resources to devote to the task, some of the resource and people are devoted to checking those with access to highly classified information; some checking those without access. If you greatly increase the amount of information that has to be compiled on those who do not have access, and you still have the same number of people, same amount of resources to devote, then that results in less attention, and a lower ability to do a thorough job on those who do have access to highly sensitive information. That's just common sense.

Mr. HOWE. Yes, Senator.

Senator GORE. If you require more work to be done on those who do not have access, then you are affecting the ability to do a good job on those who do have access.

Mr. HOWE. Yes, sir.

Senator GORE. It just seems sensible to me and was just a hold-over thought, but since you are a consultant in this area, I wanted to get your expert opinion on it.

I was very interested in your suggestions. Some of them are imminently sensible. Some of them might cause some real difficulty and controversy. And in this area, there are tradeoffs involved.

Let me ask you about one that you mentioned. The annual life event inventory profile, I am interested in how this information would be used and who would use it because there is necessarily a balance between the right of privacy and the information one must provide in order to qualify for a privilege. I take it you don't intend this recommendation to invade privacy?

Mr. HOWE. That's correct, Senator. My perception of how this would work is first to recognize all of us in the course of living go through varying periods of stress. The question is not whether we are under stress but more what we are doing about it. In this regard, I see a natural marriage here, the opportunity for a contractor to more effectively refer employees to employee assistance programs by developing the fact that an individual may be undergoing a period of stress on a temporary basis which may require some assistance. It is also saying it is to highlight the individual is going through some stress that has to be accommodated during this period. The annual review would also indicate the level and continued amount of access to classified information that the individual is having. Putting all these things together, the contractor is then in a position to better direct and target DISCO to more critical cases which should be reviewed.

I'm not suggesting the contractor undertake that review. That is the proper province of DISCO. What we are looking for is to have the contractor get involved and do screening and make better use of re-investigative resources available.

Senator GORE. That still could get a little touchy.

Mr. HOWE. Absolutely.

Senator Gore. You state that "nothing succeeds in the communication of priorities better than tangible positive demonstration of financial support." Wouldn't the kind of reward system you referred to do just that?

Mr. Howe. Yes, sir, it was mentioned a moment ago, during testimony from the Department of Energy, that some contracts do have the provision as a part of the contract a cost-plus incentive fee contract to use security performance as an incentive issue.

While the provision exists in the Federal Acquisition Regulations, to my knowledge, in consultation with my colleagues, this procedure is not widely being used. I think it goes without saying that any time a practice in industry can have a positive affect on the bottom line, it is going to get management support.

I personally would prefer and fully support the use of incentive fee contracts involving security criteria as a basic incentive. The sticky aspect of it is finding consistency in the security compliance inspections so that the criteria can equitably apply to all contractors that are involved.

Senator Gore. You would agree with the statements that I made to the witness from the Department of Energy we should have some intermediate options for disciplining companies, wouldn't you agree?

Mr. Howe. Yes, sir, I do agree and I think in effect there are some now. They may be a bit more informal, but I think they do exist. Namely, those contractors who have security interests all involved with procuring activities. The procuring activities are disinclined to enter into a contract with those contractors they feel are going to cause any form of administrative difficulty, whether it is in the compliance area having to do with procuring management, property management, personnel practices or security, so there is an incentive there, but I would agree with you it is more informal.

Senator Gore. Earlier when I asked you that first theoretical question, I said it was provoked by the last witness. I meant to say it was provoked by Mr. Devine earlier.

We are going to hear tomorrow from Christopher Boyce. One of the issues raised by his case is the fact that given our current system, he would probably be granted a security clearance again; do you agree with that?

Mr. Howe. Senator——

Senator Gore [interposing]. Obviously, if he came newly to apply and had not been convicted of a crime, that he would be granted again, wouldn't he?

Mr. Howe. Senator, I think you can take a hypothetical case where a young man came from an upper-middle-class family with a father who had served honorably in the Federal Bureau of Investigation and who was currently a security manager, a young man who was active in his church, and had a fine school background. If you had an applicant of that nature where no derogatory information was revealed, based on the premise that we stated, that past history is predictive of future behavior, in all probability, in my judgment, that clearance would be issued again.

Senator Gore. No question. But what could we do to identify someone like Mr. Boyce and what recommendations could you make to give us some kind of early warning system with a case of this kind?

Mr. HOWE. Senator, I think it is precisely the type of experience that we have had in the Boyce case that leads me to feel that we need a more proactive look at security, particularly from the standpoint of analyzing change.

A young person in their early twenties is certainly going through a period of very, very rapid change. To grant that clearance and then not look at them for a while, I think, is making a very serious mistake. I think we need to develop some mechanism for getting back in there and involving that individual in the perception that we are interested in the changes that they are going through.

Senator GORE. You indicated earlier in your statement that a fundamental problem with our system is that there is no "single industrial security posture throughout DOD." What do you mean by this, and can you cite any specific examples that lead you to believe there is some problem with this?

Mr. HOWE. Yes, Senator Gore, there was an attempt in 1965 to pull the diverse programs of the Department of Defense agencies into a Single and Consolidated Defense Industrial Security Program. In the aftermath of that consolidation, we have had the onset of a wide variety of special access programs and sensitive compartmented information activities which are conducted outside the Defense Industrial Security Program. So consequently, the contractor finds himself interfacing not only with the Defense Security Industrial Program, but all the myriad of independent special access programs plus the separate procuring activities involved with the compartmented information programs.

In our case, we would add to that the Department of Energy, Nuclear Regulatory Commission, and other elements of the intelligence community and national security community. We find ourselves, in effect, running upwards of 30 different Industrial Security Programs within an organization such as ours.

The difficult is that any one of the programs in and of itself is a fine program and makes imminent logical sense, but when you impact an employee with it, for this contract you do it this way, however on that one, you must do it this way, the result is the employee finally throws up his hands in horror and says the heck with the security stuff, you do security; I'll do the technical work.

The result is the employee feels removed from participating in the security——

Senator GORE [interposing]. They lose the respect for the importance of the procedure?

Mr. HOWE. Absolutely, Senator. We need to integrate that employee into it, and we can't do that while we are running so many different programs.

[At this point in the hearing, Senator Nunn entered the hearing room.]

Senator GORE. Again, I want to thank you for your statement and thank you for your responses to my questions.

Mr. HOWE. Thank you.

Senator GORE. I have some others. Perhaps the committee will also for the record. Thank you, Senator Nunn.

Senator **Nunn** [presiding]. Thank you, Senator Gore. Our next witness is Mr. Eli Flyer, who is a consultant, Manpower Research Center, Department of Administrative Sciences, Naval Postgraduate School, Monterey, CA.

Mr. Flyer, we are delighted to have you this morning. I understand you are prepared to give us your oral testimony, and then we will ask questions of you.

Mr. **Flyer**. Yes, and I appreciate the opportunity to appear before you today. Yesterday, we heard there may be too many classified documents. We also heard yesterday that there may be too many people with clearances. Today you are going to hear that there may be too many unreliable people assigned to sensitive jobs.

I have been a personnel researcher for Defense for over 30 years. In the early 1960's, I became involved in selection research involving assignments to high-risk jobs, positions involving nuclear weapons and intelligence duties, where espionage activities and destructive acts would have the most serious consequences.

Let me tell you what led to that involvement. In 1959, an Air Force enlistee assigned to an overseas base in Great Britain pointed a .45 weapon at a nuclear warhead. He was talked out of discharging his pistol, and it was later discovered that he had been receiving psychiatric therapy for deep depression for quite a period of time without his psychiatrist knowing about the nature of his work.

This led, of course, to quite a bit of attention being devoted by the Air Force to improving their screening for nuclear sensitive jobs. It led to the Human Reliability Program for the Air Force which later on became the Personnel Reliability Program for Defense.

After a 20-year interval, I am again involved in personnel security research. In looking over the program, I find many serious problems. Most important would be the high rate of first-term attrition of enlisted personnel due to unsuitability that is found among those placed in high-risk jobs. About 20 percent of new recruits considered for assignment to either nuclear-related or intelligence specialities who receive background investigations all discharged within the first 4 years of service for cause, largely for reasons of unsuitability. Most will have been cleared for assignment to these duties.

Senator **Nunn**. Does that mean unsuitability for those high-clearance jobs or unsuitability for the service?

Mr. **Flyer**. Let me just move into that with the next statement. Some of the people discharged for unsuitability are separated from service during early training. At the time of their discharge, many have been cleared for top secret and SCI duties. Over the last 5 years, 27,500 enlisted personnel considered for assignment to sensitive duties were later discharged for unsuitability, most had received clearances for high-risk jobs.

You asked about the nature of the discharges. Let me read you some of the numbers here. Drug-related reasons, 4,000; character and behavior disorders, 1,900; homosexuality, 1,100; alcoholism, 600; discreditable incidents, 2,800; misconduct, disciplinary infractions, 1,600; court martials, 1,100, and so on.

[At this point in the hearing, Senator Gore withdrew from the hearing room.]

Senator NUNN. What period of time is that over?

Mr. FLYER. Over the last 5 years, 27,500. And almost all cleared for high-risk jobs. What is going on?

I think it's important to recognize here that most of the adverse information obtained through background investigation relates to behavior problems rather than to loyalty issues. That point was mentioned yesterday and has to be stressed again. In selecting and adjudicating this information, it is assumed that individuals with very unfavorable background histories are poor security risks. People likely to continue having behavioral problems are more likely to be compromised.

About 5 percent of those receiving background investigations are denied clearance for high-risk jobs, and primarily for behavioral reasons—only 5 percent! Unfortunately, what the current personnel security process does not take into account is there are still wide differences in behavioral adjustment history and expected behavior among the 95 percent who are cleared.

The recruit who has been fired from a number of jobs prior to service entry is likely to receive a clearance indistinguishable from that of a fellow recruit with an exemplary preservice record, although much more likely to be discharged for unsuitability later on.

It is hardly likely that a process which identifies the bottom 5 percent of those receiving background investigations as behavior risks and everyone else as equally acceptable is providing the best candidates available for high-risk jobs.

Let me give you an example. We may have an applicant for military service who has been fired from four jobs prior to recruitment. Once because he didn't show up on time; another one because he was lazy; another one because he was suspected of theft; and another one because he was found smoking pot in the washroom. He goes to the fifth employer. The likelihood is that the fifth employer, if he does any employment checks, will turn him down, but not the Department of Defense. The Department of Defense will accept him and he will be enlisted.

If it happens that he gets into a track identified for a high-risk job and a background investigation is run, and, further, if the background investigation is accurate enough to identify these problems in his prior employment, he will probably still be cleared for top secret and for SCI duties.

I ask you, what kind of a system do we have here where an individual who is unlikely to get good employment outside Defense because of a lousy employment history will still pass muster for our highly sensitive jobs?

Senator NUNN. Are you saying the Department of Defense doesn't look into past employment records, or are you saying they disregard it——

Mr. FLYER [interposing]. I say if there is an accurate investigation and they identify the information, the likelihood is excellent that this individual would be adjudicated favorably.

I think we should look very carefully into the possibility of selecting people into high-risk jobs rather than selecting them out.

For the enlisted population, the situation may be analogous in some respects to aptitude scores for recruit selection. Aptitude batteries are applied to all applicants for military service, and only those recruits with the highest scores are considered for assignment to highly-technical positions.

Why can't we use the same approach in the personnel security screening process by obtaining assessment information from all recruits and then identifying those with the highest adjustment potential for assignment to high-risk jobs? Well, how do you do that? I believe it can be done.

Although it would be much too expensive to give background investigations to all recruits to identify those with the highest adjustment potential, we have other techniques that are less costly that provide much of the same information. Good self-report biographical history measures can provide a fair amount of the information now obtained through background investigations. For those who pass this screen, the background investigation, of course, would still be needed. This would be accomplished for the most highly qualified recruits and its purpose would be largely to check on the accuracy and completeness of the information obtained through the self-report procedures. This approach would clearly reduce the number of enlistees assigned to high-risk jobs who are later discharged for unsuitability, without question.

We are faced with the fact that there is very little information now available for evaluating and improving the effectiveness of Defense's Personnel Security Program. Dollar costs per investigation and time to complete an investigation while important are not sufficient. There are other important components of the personnel security process that could and should be evaluated to improve the program. Such as the following:

Requirements: We heard some of this yesterday. How effective are Defense policies and practices in determining who receives a background investigation?

Timing: Are prescreening procedures and background investigations being initiated at the right time? For some recruits, sometimes their background investigations are run before they are actually in service, while in the delayed entry program. Some are run while in basic training; for some while in technical training pipelines. The problem is a certain amount of fallout. Some of these people will never be assigned to a sensitive position, and this can create a fair amount of waste. One has to balance the cost of unnecessary investigations against the time spent waiting for clearances to be processed after completion of training, but this is the type of job that operations analysts do all the time in evaluating cost effectiveness.

Coverage: Is the additional background information that could be collected for evaluation purposes? I was struck hearing this morning about the comparison of 12 references versus 24 references in evaluating the quality of background investigations and kept on saying to myself, are they the right references? Did they ask the right questions? I think it takes more than just body count to determine the quality of a background investigation.

There are lots of other factors which I think should be included in a personnel security investigation that are not now included. Indicators of emotional stability, for example, are very important. I don't believe the current assessment system gets at that.

Procedures: How effective are our background investigation procedures in identifying important information in a person's background? Very little has been done to evaluate whether or not these investigations are quality investigations, whether they can actually find what's out there.

I am struck when I read background investigation records, and I have read plenty of them, that if the investigators just didn't get to John Jones, they never would have found that the subject has this or that in his background. Twelve references recommend the subject unqualifiedly, and a 13th reference all of a sudden comes up with all kinds of negative information which is later confirmed. It makes you wonder about the quality of the investigative process.

Accuracy: How reliable is the information obtained through personnel security investigations? It is along the same lines which I have been discussing.

Validity: Once you have accurate background information, what is it worth? I didn't hear anybody talk about validity in the last day or two. If you find out that an individual has committed certain kinds of offenses, had certain kinds of employment history, what does it all mean? Where are the data, where are the actuarial data that tell us the probability of later behavior associated with these things if you find them in a good investigation? We are all on very, very thin ice in terms of what we are doing from an adjudication standpoint.

Adjudicators are flying blind. They don't know the relationship between certain classes of behavior and later behavior. And then, ultimately, you have "utility." How best can personnel security information be used in making personnel security decisions? This is the reason why investigations are run. How do you take advantage of the information obtained in making effective personnel decisions? There are behavior science and operations research techniques that would help answer these questions, question applicable not only to Defense's personnel security programs but programs of other agencies as well. We need to learn a lot more about the personnel security process if our aim is to improve it and make it more effective.

We must also find ways to make up for the limitations of personnel security investigation procedures. We are faced with the fact that we cannot predict the behavior of individuals assigned to high-risk jobs with degree of precision needed. The best that can be done is identify groups of individuals with different probabilities of behavior. Based on current screening procedures, groups of recruits can be identified at service entry whose first-term unsuitability discharge rates will very from about 8 percent to over 50 percent.

While these rate could be improved to some extent, there would still be significant numbers of later failures even in the most highly selected groups. It appears, therefore, that although we can reduce the incidence of unsuitability in high-risk jobs through the use of valid selection procedures, in no case can we bring it down to zero. Incidentally, there would still be many attractive jobs left for those not assigned to high-risk jobs. That point came up earlier in terms of suitability versus security.

It's essential, therefore, to have a personnel security system that takes into account the need for continuing observation and periodic evaluation of the people assigned to high-risk jobs. A standardized monitoring and assessment program is needed with military and civilian supervisors and managers fully responsible for its effective administration.

In some respects, Defense's Personnel Reliability Program already uses this approach. The monitoring programs need strengthening in the opinion of many defense experts.

I believe we should look very, very carefully at a recertification process on an annual basis, not necessarily a reinvestigation, but involving the supervisor or the manager, to review, perhaps, with the individual in the high-risk job how things have gone within the last year, checking personnel records, checking medical records, looking for indicators that perhaps the individual today is a bit different than he was earlier.

To conclude, it's apparent that relatively little is known about the effectiveness of Defense's Personnel Security Program, or that of other agencies. The large number of unsuitable discharges among those with high-level clearances indicates that all is not well.

I believe it essential that behavioral science and operations analysis techniques to applied to the Personnel Security Program to evaluate and improve current policies and procedures, and, I believe, the effort is long overdue. Thank you.

Senator NUNN. Thank you very much, Mr. Flyer. You told me some things I did not know about the military procedures and personnel. I am particularly interested in pursuing for just a moment the analysis that these various factors, previous job problems, so forth, even if known would not prevent those people from not only becoming members of the service, but also being cleared for classified information.

Is that a policy or is that just the way it works?

Mr. FLYER. There are a set of standards that are supposed to be applied. If an adjudicator sees a consistent history of irresponsibility among other factors, then a clearance could be denied, but the illustration I gave you in a correct one, and there are probably others even more serious where clearances are given. It just would not be considered serious enough, really, for an adjudicator to turn down such an individual. I know, I have been looking at a large number of background investigations.

Senator NUNN. Does DOD do much personnel security research? You indicated you don't believe enough is being done. They do a lot of studies on personnel but do they do personnel security type studies?

Mr. FLYER. I'm not sure how much money is going into personnel research in terms of selection, utilization, promotion, retention, these types of things. Probably about $60 million a year. Large amounts are going into it. Surprisingly, relatively little in personnel security research. I think it stems from a number of reasons:

One, I don't think the managers of the personnel security programs have in the past laid out the requirements for their behavioral scientists to work on. In the last few years, there has been, I think, quite a bit of recognition, not only within Defense, but among other Federal agencies as well that there is a role for behavioral scientists to play in personnel security research.

[At this point in the hearing, Senator Gore entered the hearing room.]

Mr. **Flyer**. I think looking at the history, it's the investigators who have been running the personnel security program for a very, very long time, and I think they have done a very good job; I think they have done an excellent job, but I think there are tools available now, the tools that are common to personnel researchers, to operations analysts, to operations researchers, that would strengthen the program immeasurably.

Senator **Nunn**. Mr. Howe, I have one other question for you. You stated that you felt the security had become balkanized within the Department of Defense and otherwise. In a firm like yours, how many different kinds of security systems do you have to work with in the Government from your security point of view, and could you give us some idea what they are?

Mr. **Howe**. Yes, Senator Nunn. We are dealing with the Department of Defense in the traditional national security area, so-called collateral world, plus special access programs, plus sensitive compartmented information programs.

In the case of the special access programs and sensitive compartmented programs, the guidance and oversight on those come from the individual procuring activities themselves. So, in effect, you have a duplicative and separate interface with each one of those commands and activities. Then you can ad to that each of the other executive branch agencies that runs its own program, in our case in rough order magnitude figure I would use for our company, we are running 30 separate security programs, and in the case of separate clearances, for example, a Q clearance with the Department of Energy is not recognizable as a Q clearance with the Nuclear Regulator Commission.

I can give you a hypothetical case. Let's take a case where the Department of Defense would have a contract involving a nuclear issue, give that contract to a Department of Energy National Laboratory; that National Laboratory would receive Department of Defense information, then subcontract to a company who is a Department of Defense contractor. The DOE laboratory, in all probability, would not allow access to that DOD material unless the subcontractor went out and got DOE clearances, which gets a little absurd.

Senator **Nunn**. I agree. Both of you have been of great help to us. We hope that as we frame our recommendations we will have the privilege of getting back in touch with you and discussing some with you, including the ones you made here this morning.

Senator Gore, I am going to turn it over to you. I have been called and told the Intelligence Committee demands my presence.

Senator **Gore**. I have no questions of these witnesses.

Senator **Nunn**. We will start our hearings again tomorrow morning. We have additional testimony for today which will be put in the record, specifically that of Kathleen Buck of the Defense Department who has been most helpful. She has prepared a very thorough analysis of the legal questions involved here. We are going to, without objection, enter that into the record.

[The prepared statements of Mr. Howe, with an attachment, and Mr. Flyer, with an attachment, follow. Responses to written questions from Mr. Howe also follow:]

SAIC-85/1048

A REPORT TO THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE
UNITED STATES SENATE COMMITTEE ON GOVERNMENT AFFAIRS

"Comments On The Efficiency and Effectiveness of The Defense Industrial Security Program"

April 1985

Prepared By:

LAWRENCE J. HOWE, CPP

VICE PRESIDENT-CORPORATE SECURITY

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
1200 PROSPECT STREET - P.O. BOX 2351
LA JOLLA, CALIFORNIA 92038

REPORT TO THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS OF THE UNITED STATES SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

THE DEFENSE INDUSTRIAL SECURITY PROGRAM

The following views on the effectiveness and efficiency of the Defense Industrial Security Program (DISP) are being submitted to the subcommittee in response to a request of January 28, 1985 from the Honorable Sam Nunn, Ranking Minority Member.

INTRODUCTION

Science Applications International Corporation (SAIC) is one of America's leading research and development firms and is in active support of the national defense. The corporation has offices in 23 states including 67 separate sites presently cleared for access to classified materials under the DISP in performance through the TOP SECRET, SENSITIVE COMPARTMENTED INFORMATION levels.

The corporation presently has 4,500 cleared employees contributing to more than 350 different DoD classified contracts. This diversity of contract performance spans a wide range of technologies and procuring activities. SAIC was honored in 1984 as a recipient of the James S. Cogswell Award in recognition of an outstanding industrial security program.

In addition to the DISP, the corporation also participates in the industrial security programs of the Department of Energy, the Nuclear Regulatory Commission, and other elements of the national security community. In the interest of a more concise presentation, this paper will concentrate on the industrial security interface of the DoD.

The observations contained in this paper are drawn from exposure to contractor implementation of government industrial security programs. Additional background utilized in this presentation reflects fifteen years government service in the security field. This experience included responsibilities in personnel security administration and the inspection of contractor facilities for security compliance. A more detailed biographic profile of the author is provided at the conclusion of this paper.

The following discussion attempts to outline several issues which the author feels create obstacles to a more effective and efficient DoD industrial security posture. It is the view of the author that more uniformity and consistency of approach throughout the DoD must be achieved before significant security effectiveness improvements can be anticipated. A fundamental problem is the lack of a single industrial security posture throughout the DoD. The committee is to be commended for the breadth of the investigative approach established by the staff. A security enhancement review which concentrates soley on contractor compliance without consideration of changes to the overall institutional framework of DoD industrial security would provide only marginal improvement at best.

The presentation will begin with a discussion of some of the broader institutional issues affecting the implementation of DoD industrial security. Issues relating to personnel security concerns are treated separately in the second portion of this presentation.

IS THE DEFENSE INDUSTRIAL SECURITY PROGRAM COHERENT?

The present DISP represents a far more effective and coherent program than the one it replaced. Prior to 1965, each DoD component and agency ran its own independent program. The intent was to have heads of DoD components and agencies responsible for the effectiveness of security measures. In practice, administrative centrifugal force sent industrial security programs flying off on different vectors. Industry was faced with a confusing and contradictory assortment of procedures and rule interpretations.

The DISP developed out of a need for a more consistent and coherent interface with industry. Initially the DISP was centralized under the Defense Supply Agency (which subsequently became the Defense Logistics Agency). The Secretary of Defense became authorized to act on behalf of heads of separate DoD components and certain other executive branch agencies in matters of industrial security policy and practice. In October 1980, responsibility for the DISP was transferred to the Defense Investigative Service (DIS). This change brought better focus to the industrial security function by having the general administration carried out by a DoD component which already had security functions.

The result of all of these changes has been positive, with increased consistency, coherence and more effective quality assurance over the contractor compliance inspection process than was possible under the dispersed approach. The objective of consolidation and consistency of application which the establishment of the DISP hoped to achieve has only been partially successful. The establishment and expansion of industrial security programs within the DoD outside the DISP, has eroded the goal of consistency and coherence. The following presentation will elaborate on this position.

THE ISSUE OF INTEGRATION INTO THE PRODUCTION PROCESS

To be fully effective, security measures must be integrated into the flow of the production process. A security posture maintained separately from production is form without substance. A significant weakness in the DISP is the lack of consistency in security approaches within government procuring activities and what is expected of industry. Both elements of the procurement equation, in industry and government, are not operating under the same security rules and are not subject to the same degree of oversight.

The existence of this "double standard" is a major deterrent to an effective and integrated industrial security posture. Security practices and standards imposed on industry are far more stringent and complex than those applied to government activities. These differences include, but are not limited to, the accountability and control of classified information, reproduction controls, and the authority to hand-carry classified materials.

There are many unfortunate instances where industry comes under production pressures exerted by government procuring activities which result in the perception of a need to short-cut security procedures in the interests of expediency. This is not to imply indifference to security on the part of government procurement activities. That is not the case. The problem is one of perception. Most government personnel understand that industry has a different set of rules, but the different rules do not regulate their lives. As a result, production requirements are levied by procurement activities with inadequate sensitivity to industrial security implications. This apparent indifference of procuring activities to the DISP can erode the commitment of the most conscientious industrial employee.

RECOMMENDATION TO IMPROVE INDUSTRIAL SECURITY INTEGRATION

Both elements in the government procurement process need to operate under the same security rules and procedures. For the DISP to be coherent, it should apply equally to government as well as industry. The Defense Investigative Service should be given review and inspection oversight authority over DoD procuring activities. The resources of DIS would have to be augmented to accommodate the additional inspection responsibility.

An adjustment in the DISP regulatory framework would nave to be made. A less procedurally intensive approach would have to be found to achieve acceptance within government production elements. There is already momentum to modify the present procedurally intensive approach imposed only on industry.

The recent changes in contractor compliance inspection emphasis being adopted by DIS is sensitive to this latter point. The new inspection procedure is designed to place less emphasis on the administrative "bookkeeping" functions of security and to place more emphasis on the day-to-day "hands-on" production practices involving classified information.

IMPLICATIONS OF A MORE COHERENT GOVERNMENT INDUSTRIAL INTERFACE

CLASSIFICATION MANAGEMENT: The Contracting Officers of procuring activities are responsible to provide adequate security classification guidance to contractors. A study by the General Accounting Office (LCD-81-13, 12/16/80) stated the need to improve this classification guidance. While improvement has been noted since the report, there is still a significant variance in the ability of procuring activities to provide clear, correct, adequate and relevant guidance, especially as it relates to the security practices imposed on industry.

If oversight and review of the DISP implementation at procuring activities were to be performed by DIS, it would provide a meaningful quality assurance mechanism on classification guidance which does not now exist. By default, the "slack" has been necessarily taken up by industry, thereby requiring contractors to perform quality assurance on their own customers in order to be in compliance with the DISP. Involvement of DIS would provide access to better guidance on security requirements for contracting officers. At present, many contracts are burdened with requirements based on an incomplete understanding of the DISP by contracting activities.

OVERSIGHT AND CONSISTENCY: Commonality of practice and policy throughout the procurement cycle would insure more effective security administration. Compliance reviews which would focus on the role of the procuring as well as contractor functions would more effectively address areas requiring remedial attention. Investigative inquiry of security infractions would better take into consideration total cause and effect. The present system tends to see an incident in isolation as a contractor issue without a full appreciation of influencing factors which may have originated with the procuring activity. A further enhancement of security compliance in the procurement cycle could be achieved if the performance reviews of government procurement project managers would address the overall security posture of the project in addition to the technical and financial considerations.

IS AN EFFECTIVE OVERALL INDUSTRIAL SECURITY POSTURE BEING FRAGMENTED BY INCREASED USE OF SPECIAL ACCESS PROGRAMS?

Executive Order 12356 provides for the creation of Special Access Programs (SAP) under those circumstances where there is a need to protect particularly sensitive classified information. This requirement pertains to programs where the minimum requirements of the DISP are determined by the procuring activity not to provide adequate safeguarding mechanisms.

In practice, SAP activities have grown at an exponential rate in recent years. The General Accounting Office study (GAO/GGD-83-43, 2/18/83) cited the need for better DoD oversight of these activities. The recent revision to the DoD Information Security Regulation (DoD 5200.1-R) issued by General Stilwell, Deputy Under Secretary of Defense/Policy, concerning "Special Access Programs" represents an improvement in oversight review.

SAP programs have been implemented in a regulatory void. No provision was developed within the framework of the DISP to support or provide oversight review of these activities. In the absence of adequate centralized oversight, no new security procedural regulatory framework was developed to provide enhanced safeguarding beyond the DISP minimums. Seeking a "tighter" security framework, SAP procurement activities adopted the next available higher level of safeguarding requirements: TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION (TS/SCI). A wholesale adoption of regulations and procedures was made without apparent consideration of appropriateness.

Executive Order 12356 establishes classification levels based on a determination of the extent of damage which could be expected to be caused to the national security in the event of a compromise. Safeguarding measures are to be commensurate with an appreciation of the sensitivity of each category of classified information.

The majority of SAP activities are classified at the SECRET level. Wholesale adoption of TS/SCI safeguarding measures should not, by definition, be appropriate for the protection of information classified SECRET. This is particularly true of physical security requirements. SAP procurements are primarily justifiable on the basis of the need for a more formal control structure regulating need-to-know. The unsupervised and inadequately regulated proliferation of SAP activities has resulted, in many instances, in a misapplication of security measures.

RECOMMENDATION TO IMPROVE SAP SECURITY EFFECTIVENESS AND REDUCE THE NEGATIVE BURDEN OF THESE PROGRAMS ON OVERALL SECURITY

The DISP should be charged with the responsibility to establish uniform security requirements for all DoD SAP activities. This framework should represent an enhancement of the minimum standards contained in the present Industrial Security Regulations and Manual (DoD 5200,1-R, DoD 5220.22-R and DoD 5220.22-M). A standard tailored for SAP activities should achieve a balance between the existing minimum requirements for safeguarding classified information and the TS/SCI standards presently adopted by SAP procurement activities. Such standards should include special contracting concerns, formal need-to-know structure administration, and set reasonable physical security requirements with a special emphasis on technical security protective measures.

When there were fewer SAP activities, contractor resources were able to absorb and adequately support these special added requirements. With the proliferation of SAP procurements, contractors who are heavily involved in these activities find themselves fragmented and their resources stretched and/or depleted. The situation which has developed is not unlike the original pre-1965 days when industrial security was orchestrated by each of the separate DoD components. Requirements of SAP activities do not have sufficient commonality. Instances of arbitrary imposition of security requirements by SAP activities stem from the lack of a standardized safeguarding system appropriate for the classification level of the procurement.

Contractors are currently faced with the operation of a three-tiered industrial security system comprising DoD collateral administered under the DISP, and separate structures for DoD SAP, and TS/SCI programs. Effort needs to be expended within the DoD to bring all of these programs into a more coherent total security system. The present "Balkanization" of DoD security is an obstacle to a more effective and integrated industrial security posture.

IS THERE AN OVER-EMPHASIS ON PHYSICAL SECURITY CONCERNS TO THE DETRIMENT OF PERSONNEL SECURITY?

By all informed analysis, the weakest link in the security chain protecting our national security is the human reliability equation. Human behavior appears to consist of an infinite set of complex variables. We understand far more about the physics and chemistry of far off astronomical bodies than we do about the inner workings of our own minds.

We are able to describe with precision the amount of explosive force required to penetrate a steel security container. Charts and tables predict the number of minutes intrusion delay which can be expected by various combinations of fences and barbed wire. As yet, however, we are unable to explain why a human being does not live up to our expectations of trust.

A far greater amount of sensitive information makes its unauthorized departure from cleared facilities by walking out the door than has ever been stolen by force. Physical security measures are an essential ingredient in an overall security posture. Concern for physical security issues needs to be integrated into the overall security safeguarding posture. The question here is one of disproportionate emphasis. Given that insufficient statistical evidence exists to support requirements for measures against forced entry, an inordinate amount of resource is being expended in attempts to comply with the "steel and concrete" school of security safeguards.

Some insight into the workings of the security profession suggests some factors why this trend exists. When a loss occurs, there are demands for corrective action. Something has to be done. The subtleties of personnel security do not lend themselves to objective demonstration that something immediate has been achieved. The effectiveness of personnel security measures are more often tested over the passage of time. But add another concrete wall, weld up another plate of steel and at least something can be seen and measured.

Under pressure for action, the security profession has a tendency to quantify its delusions.

WE MUST BE MORE ARTICULATE IN FOCUSING THE PRIORITY OF NEED FOR BETTER PERSONNEL SECURITY MEASURES.

DOES PRESENT GOVERNMENT PROCUREMENT POLICY DISCOURAGE COMMITMENT OF SUFFICIENT RESOURCES ON SECURITY MEASURES?

Recent years have seen an increased emphasis on a more competitive government procurment environment. As taxpayers, we all endorse any measure which enhances quality and cost effectiveness in obtaining needed goods and services by the government. Unfortunately, the best intended measure can have unforseen negative side effects. An undesirable side effect of increased competative contract awards is on the resources available for adequate security implementation.

Present cost accounting practice recognizes security administrative expenditures as a general administrative or overhead cost of the contractor. These general "costs of doing business" are distributed across the procurements and are recognized in the rate structure approved by the Defense Contract Audit Agency (DCAA) for cost basis contracts.

There is a paradox in the case of the contractor who expends sufficient resources to implement a high quality security program. It is axiomatic that the higher the resources expended, the greater the penalty in the competitive contract arena. The contractor who reduces the impact on overhead rates by the least possible expenditure on security has a competative advantage under present contract award evaluation procedures. For this reason, contractor security managers are under pressure to meet only minimum requirements. This results in the expenditure of as little resource as possible.

RECOMMENDATION TO ENCOURAGE A MORE ADEQAUTE ALLOCATION OF RESOURCES TO SECURITY.

Contract award criteria need to be revised. Resources expended on security compliance and enhancement programs should be recognized differently from other general or overhead expenses. No suggestion is being made that government contracts be burdened with the costs of ineffective or inefficient security measures. Inefficient management or the simple "throwing of money at a problem" should not be subsidized. The position taken here is that government contract award criterea impose a penalty for funds expended on security. This practice does little to encourage resource commitment for security programs. Industrial managers misread the negative impact of security costs as a statement of government procurement priorities.

It is specifically recommended that present cost accounting practice be reviewed with a goal to establishing a means of cost recognition for security measures which is differentiated from other overhead expenditures. A security management effectiveness criteria could be established by weighting the expenditures of the security program against the overall quality of the security program. The effectiveness level could be evaluated through the present compliance inspections and the absence of incidents of consequence. Such a practice would provide positive reinforcement to those contractors who consistently demonstrate an effective security program. Nothing succeeds in the communication of priorities better than tangible, positive demonstration of financial support.

PERSONNEL SECURITY

The size of our national defense effort requires that a staggering number of people be granted security clearances. It is small comfort that so few of the people who have been cleared have betrayed this trust. Unfortunately, the amount of damage to our national security which can be caused by the failure of a single individual is so great that no statistical probability of failure rate can ever be acceptable.

Security procedures, physical security barriers, and all other external features of a security program will not and cannot of themselves prevent espionage. In the final analysis, the trustworthiness and reliability of each individual granted access to classified information can be the only effective deterrent to the loss of our vital defense secrets.

The personnel security process consists of two distinct functions; clearance adjudication and need-to-know determination. The clearance adjudication function attempts to make a predictive judgement on the probability of an individual being trustworthy and reliable. Need-to-know determination is a management assessment that the individual in question has a sufficient contribution to make to an effort involving classified material to justify his or her access to this information. Effective need-to-know determination involving defense contractor personnel should involve direct oversight by the individual government procuring activities. Clearance adjudication on the other hand is not a production related issue.

Present government practice has clearance adjudication being carried out on a decentralized basis. Within the DoD, contractor clearances which do not involve access to SAP activities, are adjudicated by the Defense Industrial Security Clearance Office (DISCO). Procuring activities involved in SAP activities carry out their own separate adjudication in connection with the granting of the access. The majority of these adjudications are referred to as "access authorizations" to avoid the issue of granting a clearance on top of the already granted DISCO clearance. Semantic debates aside, the procurement activities are engaged in requests for additional investigative background checks and adjudicative review of these findings. Whether the objective of the review is called a "security clearance" or an "access authorization," a personnel security, human reliability determination is being made.

A serious issue involves whether a centralized clearance adjudication for DoD contractor clearances might not only be more cost effective but also enhance standards and consistency. Presently, much readjudication is done which might otherwise be avoided in the interests of having a more effective job done.

I would like to now summarize a few observations about the security clearance process. Executive Order 12356 establishes levels of clearance based on the sensitivity of information to be handled. In reviewing an individual's background for higher sensitivity clearance purposes, more exacting standards are applied in interpreting the implications of past behavior. additionally, the higher the sensitivity level of the clearance, the greater amount of background information is desired by the adjudicator.

In essence, a security clearance is a finding that no grounds could be developed in the review of an individual's history which could bring his or her loyalty or trustworthiness into question. In short, although negative factors may have existed in the person's background, if not surfaced, a clearance would be approved. A fallibility in the clearance adjudication process is the degree of knowledge of an individual's background. For example, the present utilization of the so-called National Agency Check (NAC) as a basis for granting a SECRET clearance is wholly inadequate. The recommendations of the DoD Industrial Security Review Committee for the enhancement of investigative standards are entirely in order. The addition of local law enforcement agency, credit and employment checks to the NAC should significantly enhance the clearance adjudication information base. This present inadequate investigative basis for the adjudication of SECRET clearances is probably the greatest causative factor for the insistence of most special access program activities on the processing of TOP SECRET clearances to achieve a more in depth background knowledge. In many cases, this includes a full TS/SCI extended background check, even though the classification level of the particular program is SECRET.

Now a comment on some of the underlying assumptions of the adjudication process. The clearance adjudication decision is based on the same assumption that most of us use in making our own decisions about people; we generally believe that a person's past history is indicative of future behavior. While most of the time the assumption holds up, there are unfortunate exceptions. Fundamentally, the issue is change. During change, the decision-making framework undergoes modification. Factors which require a rapid change or introduce compound change can be expected to have a greater impact on the decision making framework. The greater the changes which an individual undergoes and the greater the pressure to change quickly, the lower the validity of predictive assumptions based on past behavior.

More attention needs to be directed to human reliability factors. The DoD Industrial Security Committee addressed this point as their first recommendation. The effects of change, the source of stress factors, and the implications of compound pressures of change and stress need to be better understood. The reinvestigative process needs to be more proactive rather than reactive. Effort needs to be focused on better "early warning" signs.

As a suggestion, one such mechanism for exploration might be the adoption of an annual "life event" inventory or profile. Contemporary mental health emphasis on stress management techniques utilize such an inventory to predict the probability of a stress-induced health problem. These profiles exist in various forms and are based on an assignment of numerical weighted values to a series of events which people experience during their lifetimes. The highest rated stressful event, for example, is the death of a spouse. Other events are also rated and not all of them negative. What is significant about the insights gained by these studies is the cumulative effect of a series of events which, taken separately, would have relatively low stress values. The interesting point is that an individual may be undergoing a significant amount of cumulative stress which is causing major changes in the decision-making framework although only a minimal number of the separate causative events are identifiable to outside observers.

RECOMMENDATIONS FOR THE ENHANCEMENT OF THE CLEARANCE PROCESS

STRENGTHEN THE ADJUDICATION CRITERIA DETERMINATION ROLE OF DISCO

A human factors research activity should be attached to the Defense Industrial Security Clearance Office (DISCO) to coordinate and evaluate studies of human reliability. A better understanding of human decision-making processes needs to be established. Much of the present adjudication standards take the form of a character-flaw profile. If a clearance applicant displays any of the character-flaws of a known traitor, such as a Burgess or McLean, we decide not to grant the clearance. The existing personnel security standards concentrate on symptoms (such as substance abuse, homosexuality, excessive indebtedness), without an adequate understanding of the breakdown of the personal decision process.

We live in a society that rewards innovation. In the technological environment, individuals are encouraged to question and discard traditional approaches and methodologies. Against this emphasis, we expect these same individuals to accept constraints on how they handle the information on which their innovations are based. Why does one individual accept constraints and another take the risk of violating some of our society's most important restrictions? Conscience does not necessarily make cowards of us all. The profile of a traitor may not be significantly different from that of many sociopaths and felons. Loyalty to country has become so abstract that an act of treason is not necessarily different from any other serious crime. What differentiates a traitor from a common thief may be little more than opportunity. The existing and extensive studies on criminal behavior need to be reviewed from the clearance viewpoint for insight. At present there is insufficient focus on this important resource.

ESTABLISH AN ANNUAL REVIEW TO DETERMINE NEED FOR REINVESTIGATION

The present clearance review process is structured to reinvestigate at five-year intervals for those individuals approved at the TOP SECRET level, but not at the lower levels. In practice this goal has not been adequately met because of insufficient investigative resources. Once granted, SECRET clearances do not presently receive any further investigative action unless adverse information is developed which necessitates such action. Given that clearance approvals are not truly predictive of future events, an aggressive reinvestigative effort for all clearances is essential.

Each individual cleared under the DISP could be asked to submit a brief annual update form which would highlight significant changes which occurred during the past year. The survey should include a signed restatement concerning each of the issues covered under the present Personnel Security Questionnaire, Part III, the so-called "privacy section," which deals with suitability issues such as arrest, medical/financial and questionable organizational affiliations. The survey could be supplemented with a modified form of the stressful event inventory discussed above.

These annual updates could be screened by the contractor's security manager prior to submission to DISCO. Those statements reflecting questionable activity or a significant amount of stress/change factors could be identified for more immediate DISCO adjudicative review. Based on these inputs, better focus could be given to reinvestigative efforts. The necessity to participate in an annual update would also reinforce personnel security awareness among cleared personnel.

To effectively carry out the pre-screening function, contractor security personnel would have to be afforded access to the so-called "privacy portion." This leads to the next recommendation.

GRANT CONTRACTOR SECURITY PERSONNEL ACCESS TO THE PRIVACY PORTION OF CLEARANCE APPLICATIONS

The underlying objective in this recommendation is to involve the contractor in a more active and conspicious personnel security role.

The present policy and practice of the DISP is to prohibit access by contractor security staff to the "privacy portion" of security clearance applications. The issues raised in this portion of the personal history questionnaire relate to activity which might be judged unsuitable for favorable clearance adjudication. The reasonable rationale for excluding contractor representatives from this information is the assumption that a "chilling effect" on the responsiveness of the applicant might occur.

While the DISP position has merit, on the face of it, another significant factor has not received adequate consideration. The practice establishes a contradiction in the mind of the cleared contractor employee. During the clearance application process, the employee is given to understand what is explicitly none of the contractor's business. Then during the security briefing process the employee is told to come and report to the contractor's security department "adverse" information about themselves concerning issues covered by the privacy portion. Categorically, this is a mixed message.

Involvement of qualified contractor security personnel in the completion of the form dealing with these issues is more likely to insure a better understanding on the part of the applicant. Knowledge that significant issues exist in the background of the employee which suggest that a clearance might not be appropriate could halt the clearance application process before it gets started, thus saving important government investigative resources. The function of the contractor's security staff needs to be upgraded to a more active and proactive role in personnel security considerations.

UTILIZE INTERVIEW TECHNIQUES ON ALL CLEARANCES SECRET AND ABOVE

The DIS has indicated a significant increase in developed significant information since the adoption of the interview augmented background investigation. Less productive investigative techniques, such as effort expended in applicant neighborhoods more than five years after the last residence, should be dropped in favor of direct subject contact. This practice has been utilized to date in DoD TOP SECRET clearance investigations. This procedure should be expanded to include all SECRET clearances. In this regard, personnel security investigative standards affecting SCI access under DCID 1-14 should be reviewed in light of the positive results of the DIS approach.

CONSOLIDATE ALL DOD INDUSTRIAL CLEARANCE ADJUDICATION AT DISCO

As stated earlier, DoD components involved in SAP or SCI procurements carry out clearance adjudication. It is entirely appropriate for procuring activities to make judgements concerning need-to-know. The judgement of the necessity for an individual to contribute to an effort is best made as close to the procurement activity as possible. The duplication of clearance adjudication activity is another issue.

DISCO should have a special adjudication section established to handle the eligibility for clearance of all DoD contractor personnel requiring access through TS/SCI. Director of Central Intelligence Directive (DCID) 1-14 has established the minimum standards for the entire national security community which must be met to grant clearance and access to TS/SCI. The establishment of a centralized point for all DoD contractor adjudication, including all SCI activities, would insure a higher level of consistency and afford a more informed basis for DoD recommendations of new clearance adjudication criteria.

A DISCO section concentrating in DCID adjudication could be readily equipped to accept clearance action requests from all DoD components without jeopardizing the sensitivity of any activity. In fact, the handling of all such access approvals under a single procedure would eliminate the "uniqueness" of some present processing approaches.

The transfer of existing personnel slots involved in non-DISCO clearance adjudication to disco would, in all probability, be more than ample to handle the processing requirements without any overall negative defense budget impact. Beyond question, some economies of scale should be anticipated.

FURTHER EXPAND THE ADJUDICATIVE STANDARDS DETERMINATION ROLE OF DISCO TO INCLUDE FORMULATION OF REQUIREMENTS FOR SAP ACCESS.

Executive Order 12356 provides a basis for establishing Special Access Programs under those circumstances where there is a need to protect particularly sensitive information. The establishment of an SAP activity is deemed justified based on a determination that the minimum standards for safeguarding classified information under the DISP are not considered adequate.

Having determined that additional safeguarding measures are necessary for SAP related materials, no consolidated or consistent standards for enhanced personnel security were developed. As a result of this void, an inappropriate wholesale adoption of DCID 1-14 access requirements has been made by many programs.

Because of this void, a need exists to establish clearance adjudication criteria to reflect a sensitivity level beyond that required for a SECRET collateral clearance and less than the DCID 1-14 standards established for TOP SECRET SCI access. An intermediate adjudicative base for more sensitive access could be developed reducing the present high cost and manhour delays involved in the requirement for a full 15 year extended background investigation to SCI standards which some programs have required.

At present, much unnecessary readjudication is done on SCI and SAP activities. Significant savings and hopefully enhanced uniform standards could be achieved by a common, central special-access adjudication authority. With the establishment of a centralized clearance adjudication capability, procuring activities could be restricted to doing only need-to-know determinations.

SHOULD PRESENT POLICY BE CHANGED TO PERMIT THE GRANTING OR CONTINUED HOLDING OF A SECURITY CLEARANCE TO BE A CONDITION OF EMPLOYMENT?

Present DoD industrial security policy as stated in the Industrial Security Manual, prohibits the use of a clearance as a condition of employment. Several problems are involved in this restriction. Many firms are involved to a major extent in defense related activities which require clearances. The inability of an employee to meet government clearance criteria is beyond the control of the employer. Present policy burdens industry with the retention of personnel who do not meet an essential qualification necessary for the performance of duties for which they were hired. A second and important factor involves the perception on the part of the employee on potential sanctions for failure to adhere to security procedures.

The DoD security clearance indoctrination procedures call for familiarizing the employee with the provisions of Title 18, U.S. Code. The employee is warned of possible prosecution under Title 18 for violations under the act. In practice, successful prosecution under Title 18 for national security related offenses is so rare as to be an endangered species. Any perception of vulnerability under Title 18 by the average employee is all but remote.

A legislative and policy review needs to be made to establish a basis for an employer to make a clearance a condition of employment. A legally supported basis to establish this condition would deliver a very effective message. The loss of a clearance by an employee based on a history of disregard for security procedures or other serious misconduct, would also be the basis for a prompt, justifiable termination of employment. That cause and effect chain is far less remote than potential prosecution under Title 18. The closer the coupling of the sanction with the act of noncompliance, the more effective the sanction becomes in behavior modification.

It can be speculated that a basis for present policy may very well lie in the inability of current security clearance adjudication procedures to meet due process requirements. Clearance adjudication must be able to meet standards for uniformity and not appear capricious or arbitrary. If present clearance practice is unable to meet these requirements, it is encumbent upon the government to correct the problem and not have the burden born by industry through retention of individuals who are denied clearances.

A LEGISLATIVE AND POLICY REVIEW SHOULD BE CARRIED OUT TO ESTABLISH A LEGAL BASIS FOR A CONTRACTOR TO MAKE A SECURITY CLEARANCE A CONDITION OF EMPLOYMENT.

IN PERSPECTIVE

The recommendations and observations which this presentation makes to the Subcommittee are broad and sweeping in their scope. They are being presented with an appreciation of the "territorial imperatives" and organizational inertia which accompany major changes in government procedures or organizational charters.

It is recognized that some of the goals and objectives outlined in this discussion may present significant problems of implementation. It is also recalled that significant resistance had to be overcome in the 1965 consolidation of DoD industrial security oversight into a single DISP.

In summary, the intent of this presentation is to encourage a broad review of DoD industrial security interface, with a goal toward identifying more effective long-term solutions.

THE AUTHOR

Lawrence J. Howe is the Vice President for Corporate Security for Science Applications International Corporation (SAIC). Mr. Howe has functioned as the senior manager for security at SAIC for the past seven years. Prior to joining the corporation, he completed fifteen years service with the CIA. In his most recent assignment, he functioned as a Regional Industrial Security Officer with oversight responsibility for more than 162 contractors. He was a participant in that agency's investigative review of the Boyce-Lee espionage case. His other CIA experience included personnel security assignments, overseas operational support, and conducting polygraph interviews. The DCI awarded Mr. Howe a Certificate of Distinction for Courageous Performance.

The author is active in professional societies and is a Certified Protection Professional (CPP) of the American Society for Industrial Security (ASIS). He is the current Chairman of the Standing Committee on Government Security of ASIS and is past Chairman of the San Diego Chapter of the society. He is also active in the National Classification Management Society, the Research Security Administrators, and the Industrial Security Working Group.

His educational background includes an undergraduate degree in geology and graduate work in political science. Mr. Howe and his family make their home in San Diego.

APPENDIX

The following commentary appeared in the SAIC internal newspaper, The Newsgram. At the request of the subcommittee minority staff, a copy is being provided as an appendix to this position paper.

THE FALCON AND THE SNOWMAN

a commentary by Larry Howe

In 1977, an espionage case involving a major defense contractor burst into the national awareness. The case of Christopher Boyce and Daulton Lee was made all the more sensational by the subsequent escape of Boyce from federal prison and his recapture some eighteen months later. The book, The Falcon and the Snowman, by Robert Lindsey stirred controversy from what some felt an overly sympathetic treatment of Boyce given the extent of damage which resulted from his sale of defense secrets to the Soviet Union.

The film adaptation of the book is currently being seen in local theatres. Those familiar with the book will recognize liberties taken in the film with the intent, one supposes, of making the screen version commercially viable. The heavy hand of Hollywood is all too apparent in some of the more obvious hyperbole such as a cocktail mixing document shredder and a Smith & Wesson toting Director of Security.

Beyond the hyberbole, the story is about the real personal and national tragedy of espionage. Although the actual incident occurred almost ten years ago, the same fundamental questions are still being asked. How could it have happened and how could such an incident have been prevented?

Regardless of the security measures in place in the contractor's facility, the espionage breach would not have occurred if Boyce had not made the decision to carry it out. Postmortems on the security procedures of the contractor are distractions from the central point. In the final analysis there was a breakdown of individual integrity and responsibility.

One naturally asks how a person like Boyce got a clearance in the first place. In reality, if another individual were to submit a clearance application with the same background and history which Christopher Boyce presented, the probability is a clearance would again be granted. A clearance decision by the government is based on an assumption that many of us use in making our own judgements about people; we generally accept that a person's past history is indicative of probable future behavior. While most of the time the assumption holds up, there are exceptions. People change, and as they change their decision making framework undergoes modification. Therein lies a central weakness of the security clearance process.

In the study of Boyce we become aware of a paradox. Boyce is portrayed by author Lindsey as an intelligent, sensitive individual who becomes dissillusioned at what he feels are deceitful and covert acts of self interest by the government. This perception apparently justifies, in Boyce's mind, deceitful and covert acts in his own self interest.

Recalling the mid 1970's, there were feelings of disillusionment left by the post Vietnam and Watergate experiences. At another time with less suspicion of government, would Boyce have gone to such extremes in response to his own disillusionment? Many of us come to the story of Boyce hoping for explanations. We don't find simple solutions because there aren't any. Boyce's legal defense at his trial attempted to place responsibility outside of himself for his acts. With all of his attempts to provide external justification, he failed to explain his willingness to accept payment of twenty thousand dollars for treason. Interviews with him subsequent to his recapture convey all too clearly the contempt with which he holds the values of our society.

Perhaps the most compelling question of all raised by an espionage case is, will another Boyce turn up in our midst? Will someone else have the distorted sense of self to make a decision against the welfare of the nation? The disturbing reality is that we have little assurance that it can't and won't happen.

Security procedures and systems are at best deterrents and reminders to the honest to stay honest. This external structure is not in and of itself the answer to the prevention of espionage. In the end, personal commitment to integrity and acceptance of individual responsiblity will be the only effective deterrent.

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * *

LAWRENCE J. HOWE
Vice President-Corporate Security
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

Q. What do you mean on page 5 of your statement that the "unsupervised and inadequately regulated" Special Access Program activities has resulted, in many instances, in a "misapplication of security measures"? Can you give us examples?

A. The proper application of security measures utilizes safeguarding features appropriate to the classification level of the information involved and administrative controls for need-to-know. A Special Access Program, by definition, requires more stringent need-to-know administration. More formalized review and approval procedures are employed before access approval is granted to specific program information.

Executive Order 12356 defines three levels of security classification based on the extent of damage to the national security which could be anticipated through unauthorized disclosure. These levels are the familiar CONFIDENTIAL, SECRET, and TOP SECRET. Implementation instructions derived from the Executive Order specify measures appropriate to properly safeguard each level of classified information.

The majority of DoD Special Access Programs are classified at the SECRET level. In the absence of a unified DoD implementation instruction for Special Access Programs, a regulatory vacuum has developed for an enhancement of safeguarding beyond the minimums established in DISP. As a result, procuring activities, which as a rule do not have experienced security staffs attached to their organizations, adopted the next available enhanced safeguarding guidelines within the DoD. These measures are outlined in DIA Manual 50 - 3, Physical Security Standards For Sensitive Compartmented Information Facilities. With only rare exception, Sensitive Compartmented Information is classified TOP SECRET. A significant number of DoD Special Access Programs have specified the DIA Manual 50-3 as the physical security standard applicable to the procurement. Through this practice, an "institutionalization of overkill" has taken place on DoD Special Access Programs.

Two specific examples of physical security requirements may illustrate the incoherence which has developed between the DISP and Special Access Programs.

-Alarm Requirements: By utilizing the DIAM 50-3 as a baseline document, Special Access Programs require the installation and use of a high security alarm system capable of being responded to within 5 minutes for SECRET level material. Under the DISP, TOP SECRET material is alarm protected with an alarm response time of 15 minutes. SECRET material stored in approved safe containers, requires no alarm protection under the DISP.

-Facility Construction Standards: Special Access Programs utilize the DIAM 50-3 requirement for segregated and dedicated workspace wherein the perimeter walls have been modified to establish a sound transmission attenuation level of at least 45 db. The DISP has not imposed this requirement even for TOP SECRET material. It is again recalled that most all special access materials are classified at the SECRET level.

In the personnel security area, Special Access Programs have registered their lack of faith in the issuance of a SECRET clearance soley on the basis of a National Agency Check by having required TOP SECRET level background investigations. It is apparent that for some time DIS was unable to explain the increases in TOP SECRET clearance investigations without evidence of a corresponding increase in TOP SECRET procurements. DIS subsequently sought and achieved a tightening of justifications for the use of background checks on SECRET level procurements. To circumvent the tightening requirements, the response of many Special Access Program procuring activities was to ask contractors to identify an existing TOP SECRET contract then in performance at the contractor's facility. This TOP SECRET contract is cited on clearance applications as the basis for the background investigation rather than the SECRET level contract on which the individual was actually to perform.

The objective of my testimony was not to lower Special Access Program requirements to those of the DISP minimums. My recommendation was to have uniform enhanced standards developed for use by all DoD components involved in Special Access Programs. A reasonable and justifiable enhancement of security safeguarding should be achieved between the DISP requirements for SECRET without utilization of TOP SECRET standards.

QUESTIONS AND WRITTEN RESPONSE/HOWE-SAIC

Q. It has come to our attention that there are no uniform standards for investigation or adjudication of personnel within the Government. Should a Commerce Department employee be subject to a different standard of investigation than a DoD employee or contractor employee if they are all having access to a similar level of classified information?

A. To first respond to the question, the answer has to be an obvious no. The statement of general adjudicative criterea applicable for security clearance purposes was set forth in Executive Order 10450. The Executive Order was somewhat less specific on establishing uniform investigative procedures and standards. As a result, investigative elements within Government have a degree of latitude in establishing their own standards and practices. This disparity in investigative practices has caused reinvestigations of currently cleared individuals by agencies who consider the initial investigation flawed.

An example of the variance in investigative standards was indicated during the recent public testimony before the Subcommittee. One of the witnesses asserted the superiority of the investigative product of his element on the basis that their investigations showed a higher number of sources. With due respect to the witness, numbers of sources may not be the most significant issue. For example, 10 sources contacted telephonically in an apartment house given by the subject of the investigation as an address some 10 years earlier might not yield 10 significant sources.

As indicated above, some agencies re-run portions of investigations already done if the indicated methodology does not meet the standard on the second agency. Some non-DoD agencies will not accept portions of background investigations where sources were not contacted in person. Telephone contact with sources is generally regarded as having marginal validity.

Executive Order 10450 while still the applicable basis for general adjudicative standards, is regarded by most as dated. The absence of more recent standards representing inter-agency concensus has led to a reinterpretation of the adjudicative criterea on an agency-by-agency basis.

My testimony sought to address this issue by beginning with the DoD contractor clearance framework and seeking a consolidation of adjudication standards and practice. The next step would be to apply the consolidation to all DoD clearances. Finally, implemention of such a program among the other Executive Branch components could be attempted.

Q. What happens to one of your employees if he's rejected for one project when he already holds the same level of clearance granted for another project? Are you advised of the reasons for the denial? What can you do with the information?

A. For the purposes of the question, it is understood that the individual is being turned down by a Special Access Program where adjudication is done outside of DISCO. Under the DISP, DISCO would have an established mechanism for due process review and appeal. Special Access Programs have little of the former and none of the latter.

Government related activities seem to exemplify the proposition that institutions have both formal and informal structures. By most accounts, the informal structure tends to be the more efficient in terms of production. The point is that under the formal procedures, the interpretation of Privacy Act considerations constrains Government clearance adjudicators from revealing to contractor's the nature of the reason for clearance or special access denial. Without knowing the reason for the denial or, in most cases whether the matter was to be shared within Government channels, contractor security managers are powerless to do anything.

In those instances where the contractor has a professional security manager who is recognized by the Government element involved and a spirit of rapport has been established, "informal" communication takes place after a denial. Even in these cases the contractor is rarely given detail. Cryptic indicators are shared to give the contractor some basis for understanding the gravity of the denial. At best, the "informal" relationship might reveal whether the matter was of sufficient gravity to be shared with other clearance elements or even possibly with law enforcement agencies. That information at least provides a better understanding on the part of the contractor to what his responsibilities under the circumstances may be.

It is my judgement that an informed review of Privacy Act provisions is in order to work toward a more consistent and effective basis of joint cooperation between Government and industry in "problem" personnel security cases.

Q. Do you even know who is doing the adjudications for these Special Access Programs and what standards they're using? Doesn't this proliferation of separate projects lead to situations wherein separate agencies will conduct investigations on the same employee; as well as separate adjudications for the same level of clearance?

A. For the most part, contractor security staffs are only the conduit between the individual and the Special Access Program office which receives, evaluates and adjudicates the clearance/access approval authorization. Contractors are not part of the adjudication process.

The thrust of my testimony in this area was to call for the establishment of a specific set of enhanced standards over those used to grant a DISCO SECRET but less demanding than DCID 1/14 for use on all Special Access Programs at the SECRET level.

The growth of separately administered Special Access Programs within the DoD has lead to much duplicate adjudication. In my judgement, this is unnecessary and wasteful. To this point, my testimony recommended the centralization of all DoD Special Access Program adjudication affecting contractors at DISCO. As I would envision the concept working, Special Access Program offices would make a determination that a contractor employee had sufficient need-to-know to justify the access. Having made that determination, the Special Access Program office would query the centralized adjudication database at DISCO and request a determination that the individual's current clearance status was adequate to meet the enhanced, uniform standards discussed above. The Special Access Program office would be entitled to receive either a "yea" or "nay" only. Their role would be confined to determining need-to-know only and to have DISCO make the personnel security adjudication determination.

The problem of lack of commonality and interchangeability is not confined to Special Access Programs. A "Q" access approval which meets Executive Order 10450 criterea for access to TOP SECRET is not interchangeable between the DOE and NRC. At least the DoD will accept a DOE "Q" as a basis for conversion to a DoD TOP SECRET. The DOE, however, will not honor a DoD TOP SECRET.

Multiple agency participation in contracts creates a nightmare for industry. Not only are the security practices different but the clearances are not interchangeable. For example, a DoD classified document forwarded by a DOE component would require a DOE clearance for access by one of our employees although the individual was already cleared by DoD.

QUESTIONS AND WRITTEN RESPONSE/HOWE-SAIC

Q. Do you think industry should take a larger role in pre-screening employees for clearances?

A. Privacy Act considerations constrain most companies from attempting more than a cursory background check of employees. Checks made of applicants of past employment usually not yield more than an acknowledgement that an individial had been employed and fewer will state whether the individual is eligible for rehire. Smaller companies cannot afford to either establish an investigative capability or to pay the "head tax" to use commercial outside resources. I would personally be concerned about the uniformity and quality of the background screening check done from one company to another.

In my testimony I made a suggestion to involve the security departments within industry in a more pro-active role in the clearance screening process. I pointed out that current interpretations of the Privacy Act and DoD policy (more the latter than former) restrict contractors from having access to that portion of clearance applications dealing with suitability issues. I feel this is a serious mistake. Contractor security personnel could review these issues with prospective candidates for clearance in a manner which would insure better understanding of the issues and screen out those individuals on whom a background check would be a waste of time and manpower.

QUESTIONS AND WRITTEN RESPONSE/HOWE-SAIC

Q. On pages 2 and 3 of your prepared statement, you raise the issue of a "double standard" between industry and government. Do you have any concrete examples of this? How does this affect your role in corporate security?

A. At the outset, I would like to reassert that I am not suggesting an indifference on the part of procuring agencies to security. The difficulty is that whenever two sets of rules govern the same activity, production expediency will favor implementation of the more flexible or less restraining rules.

This can be illustrated in a scenario of an interaction between an individual on the production side within a procuring agency and his counterpart in industry. During contract performance there are numerous contacts and sessions to assess progress and iron out problems. When the government side comes to visit the contractor, he is realatively free to reproduce whatever material he feels will be useful for the discussion, place it in an envelope in his briefcase and appear at the contractor's site. No rigid document accountabiity has taken place and no log out or transmittal receipt system has been used. Once at the contractor's facility, the government representative may choose to leave some of the material in the hands of his industry counterpart as it is found germain to the production issues being discussed.

The next day, on short notice, the government side invites the industry counterpart to come to the agency and discuss some matter that came up the day before. With less than two hours notice, the industry side is asked to prepare some "viewgraphs" of some of the issues covered the day before to be used in an informal briefing. This scenario seems uncomplicated and is commonplace.

The differences in regulation and procedures create the following snags. In the first instance, industry finds itself in possession of classified materials which did not come into the facility through established channels. This in itself is technically reportable to DIS. The industry technical staff member has a problem. If he surfaces the material to his own security people they may react by the book and demand to know who brought it in and how it got there. This puts the industry technical staff member in the position of "blowing the whistle" on his own customer. Most industry people would see that as an act of instant self destruction. The other alternative is to not inform the security staff and to attempt to conceal the material because it is technically out of accountablity. That is common within government but prohibited within industry.

In the second part of our scenario, the industry side finds itself having to carry out reproduction and new document generation with very short time constaints. The generation of "working paper" documents within government is handled with a great deal of flexibility. Under the industry rules, elaborate accountability and document number procedures are required both for reproduction and the transmittal of the material outside the facility. Given the short time constraints, in all probability the industry side will generate the documents, put them in a briefcase and go to the meeting with the intent of "catching up with the bookkeeping later". In some instances, later never comes because there are new production requirements.

In this very typical example, the industry technical staff member has committed a series of security violations which are not violations for his government counterpart.

The effect of this double standard upon security management within industry is to create an almost unbridgeable gulf between security and the production side of the house. Technical staff members feel they are being responsive to their government customer who sets the tone of how production will be carried out. If the customer can freely reproduce material and hand carry it, he expects the industry side to do the same. The industry security manager attempts to have the government rules apply within the facility but the government isn't operating by the same guidlines.

The present system places all responsibility for failure to follow the rules on industry. The expectation that industry will "blow the whistle" on their own customers, particularly in an increasingly competitive procurement climate, is totally unrealistic.

My testimony sought to address this problem by involving DIS directly on both sides of the equation. It will also be necessary to strike a less procedurally intensive approach to document accountability to have a truly integrated and consistent security practice.

QUESTIONS AND WRITTEN RESPONSE/HOWE-SAIC

Q. As you are aware, since 1978 through the establishment of the Information Security Oversight Office, we have a semblance of uniformity and consistency in the handling of classified documents. Don't you find it ironic that we have no consistency in the handling of personnel security issues affecting employees who handle these documents? In your opinion, do you feel we need some oversight office for personnel security just like we have for information security?

A. I seriously question the utility of a personnel security oversight office. The information security oversight function makes a case in point. I have the highest personal and professional regard for Mr. Garfinkle. The problem he faces is the magnitude of the job with the resources at his command. If I may be forgiven an analogy, it is like being tasked to follow the circus elephant parade equipped only with a dust pan and whisk broom. There is more activity out there than can be effectively handled.

The review capabilities and sanction power of the Information Security Oversight Office limits their ability to make a really substantial impact. The degree of consistency in information security which may appear to exist is largely in those clear cut issues which subject themeselves to "black and white" regulatory issuance. Under the surface, there are a whole range of classification management issues which are not being handled consistantly simply because of the lack of true centralization. That again is not a criticism of either Mr. Garfinkle or the ISOO staff. The manner in which their role is structured prevents them from being more effective.

My strong recommendation to the Subcommittee is to seek centralization of clearance adjudication rather than impose another layer of essentially powerless review.

A centralized clearance adjudication function offers more hope of implementing unified clearance adjudication standards than the present dispersed system. I would have the clearance investigative element supporting the adjudication process part of the same agency but under a separate management structure. Investigative information gathering must not engage in de-facto adjudication by selective reporting. The investigative resources need, in my judgement to be responsive to the same agency head to insure effective communication of feedback and corrective action if the investigative product is not providing the adjudicative function with adequate information.

QUESTIONS AND WRITTEN RESPONSE/HOWE-SAIC

Q. In light of your testimony on the various security systems you must operate under, I can appreciate your phrase that security has now become "Balkanized". Just for clarification purposes, how many different security systems does a medium size firm like yours have to work under? Does each one have different requirements? What is the major problem with operating under all these different systems?

A. Within the DoD procurement interface, there are 3 generic systems; the collateral program under the DISP, the various Special Access Programs, and the Sensitive Compartmented Information areas. Both the Special Access Program and Sensitive Compartmented Information areas have as many subsets as there are separate contracts.

The DOE and NRC make another generic pair of systems. In the DOE context, each of the 7 operating regional offices functions on essentially an autonomous basis. We have often been inspected separately by different operating offices of the DOE on the same effort.

Currently, we are operating under some 30 different security cognizant authorities.

The major problems with this condition are the difficulties of administering a coherent security program with the variations in rules and interpretations, the dilution of our recourses, and the credibility of security procedures in the minds of our employees. In my judgement, the latter is the most damaging. Most employees feel that government security practice has become a rabbit warren of confusing rules and procedures. The average employee looks upon security as something the security staff is hired to keep straight while they are divorced from the process. The common watchword is "you do security and I'll do the technical work"! This lack of integration of security into the work process is one of the major vulnerabilities in current industrial security practice.

QUESTIONS AND WRITTEN RESPONSE/HOWE-SAIC

Q. What do you feel is the biggest problem with our Government's current personnel security system? What can be done about it?

A. As I indicated in my formal testimony, I see three major issues which relate to personnel security effectiveness: enhanced adjudicative standards; consolidated adjudicative processing, and commitment of resources to aggressive reinvestigation.

In the area of adjudicative standards, it is my recommendation that a "human factors" or "human reliability studies" function needs to be consolidated within the DoD, such as at DISCO, to review and initiate research in these vital areas. Our present adjudicative standards lack consistency and credibility because of the lack of a sufficient scientific validity for their base. The character flaw inventory approach reflected in Executive Order 10450 is not adequate to our needs for meaningful standards.

With regard to the adjudicative process, as long as the process is carried out on a dispersed basis, it is impossible in my opinion, to develop either the consistency or the base of professionally qualified personnel to carry out this function. Consistency and better attention to quality review could be better achieved, in my view, with a consolidated organizational structure tied into the adjudicative standards development and review function.

STATEMENT OF

ELI S. FLYER
CONSULTANT, MANPOWER RESEARCH CENTER
DEPARTMENT OF ADMINISTRATIVE SCIENCES
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

BEFORE THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

APRIL 1985

I would like to thank members of the Subcommittee for providing me with the opportunity to appear today and to present my views on personnel security matters. I will be making a number of observations and recommendations to improve the personnel security process. Since these are in large part based upon my experience as a personnel researcher, I would like to describe some of the projects and findings that have helped shape these views.

In performing research for the Department of Defense over the past thirty years, I have had the opportunity to work on many important manpower projects and issues. One of the most important was an Air Force project in the early 1960s to improve screening procedures used in assigning personnel to high-risk jobs. Afer a twenty-year interval, I am again deeply involved in a personnel security research effort, this time under the auspices of the Naval Postgraduate School in Monterey, California.

My interest in improving selection procedures for high-risk jobs goes back to the late 1950s and early 1960s when I was with the Air Force Personnel Research Laboratory at Lackland Air Force Base, Texas. The Air Force had introduced a major quality control program designed to discharge enlisted personnel not able to meet Air Force behavior standards, and I initiated research to reduce the problem by improved screening prior to enlistment. A wide variety of personnel assessment data were collected for a very large number of recruits, and follow-up studies were conducted to determine the validity of the information in predicting unsuitability discharge. It was through this research that high school graduate status, age at enlistment, and Armed Forces Qualification Test scores were first identified as predictors of first-term attrition for unsuitability.

Many of the research studies performed during this period were massive in scope. For example, one study involved over two-hundred-thousand Air Force recruits who were followed during their first four years of service. Aptitude, biographical, interest and attitude data were collected for assignment purposes shortly after service entry. These data were related at a later date to behavioral criteria obtained during initial enlistments. The study demonstrated that it was possible to combine many of the biographic, interest and attitude items into scales that would differentiate between enlistees with normal separations and those experiencing behavioral and adjustment problems during military service.

During the early 1960s, I also became involved in research to develop suitability screening procedures for assignment to high-risk jobs -- positions such as nuclear weapons and intelligence duties where destructive acts and espionage activities would have the most serious consequences. These were jobs requiring Top Secret and other high-level clearances based on background investigations. Using Air Force records, I was able to identify and follow-up about two-thousand recruits assigned to munitions and weapons duties after their enlistment. Ten percent of this group was discharged for unsuitability during the first two-and-a-half years of service. Personnel records were obtained and examined to see if there were preservice indicators of an individual's later behavioral problems during military service, and to obtain more detailed reasons for the unsuitability discharge.

Analysis of the data showed that it was possible to improve the selection criteria then employed for assignment to nuclear-related occupations. It also showed the necessity for on-the-job monitoring activities to identify and remove airmen with behavioral problems from sensitive duties. The final report of the study recommended the use of special procedures in selecting recruits for high-risk jobs. For example, it was recommended that recruits be high school graduates, have an acceptable level of general intelligence, and have received favorable peer evaluations during basic training. It was also recommended that enlisted personnel assigned to special weapons duties be screened more thoroughly through a continuing program for suitability evaluation on the job. This research effort led ultimately to the development and implementation of the Air Force's Human Reliability Program, later subsumed by the Department of Defense (DOD) Personnel Reliability Program.

The screening procedures introduced at Lackland for recruits being considered for assignment to high-risk jobs (intelligence as well as nuclear-related) were quite elaborate. The evaluation consisted of a questionnaire completed by the recruit to identify preservice behavior problems, a personal interview, peer ratings for responsibility and emotional stability, and educational and employment reference checks to provide some of the information usually obtained during a background investigation. Based on a review of this information, recruits with a history of serious behavior problems were diverted to less sensitive occupations.

Much of the research performed at Lackland during the early 1960's to improve screening for high-risk jobs remains unpublished. A number of these studies are worth highlighting here. One study was designed to test the accuracy of background investigations in developing significant behavioral information. A special survey administered to over twenty thousand basic trainees at Lackland was used to identify a group of fifty airmen with serious behavioral problems such as police offenses, psychiatric treatment, and poor educational and employment history. With the cooperation of the recruits involved and the Air Force Office of Special Investigations, (which conducted background investigations in that period), background investigations were initiated for the fifty airmen. The size of the group was kept to fifty in order to keep investigation costs to a minimum. Results from the completed investigations showed that no derogatory information was found in about half of the cases. These "misses" can probably be attributed, in part, to the field investigators not contacting the most knowledgeable references and not asking the most pertinent questions.

Another study was designed to examine the predictive validity of information obtained through background investigations. Data were available for about twelve-thousand Air Force enlistees whose background investigations revealed derogatory information. These data were categorized and then related to later discharge for unsuitability. Comparisons with control group data showed significant relationships between the derogatory information and subsequent attrition from service. Additional analyses showed that the more serious the derogatory information, the greater the probability of being discharged at a later date for unsuitability. It is believed that these data provided the first empirical evidence of the validity of background investigation information in predicting subsequent behavior.

Another unpublished but important study involved a review of investigative records for a large number of Air Force officer and enlisted personnel who had committed suicide. Of specific interest here was whether or not the self-destructive acts were preceded by behavioral indicators -- a matter of considerable importance for the Personnel Reliability Program. Intensive interviewing conducted by the Air Force's Office of Special Investigations with relatives and coworkers showed that about half of the suicides that occurred were not foreshadowed by observable behavioral signs. This finding indicated that it would not be possible to rely exclusively on the recognition of behavioral indicators by family, supervisors or coworkers in identifying those individuals about to commit this type of self-destructive act.

Favorable findings from the prescreening research project at Lackland led to the operational implementation of the program during 1965. There had to be resolution first whether or not prescreening for high-risk jobs was part of the personnel classification process for recruit assignment or part of the personnel security investigation process. It was finally concluded that the prescreening program would be less controversial if carried out as part of the personnel classification process. This assessment program still exists at Lackland with a number of modifications.

Today, in looking once again at the Defense Department's Personnel Security Program, and more particularly at the investigative process used in assessing people for high-risk jobs, I find that a number of important and useful changes have been made. Background investigations are now conducted by a single agency, the Defense Investigative Service, rather than by the Military Departments, and centralized adjudication of background investigation information has become the norm. Some of the effects of our earlier research efforts can also be seen: the Personnel Reliability Program, recruit prescreening for high-risk jobs, and the use of subject interviews as part of the background investigation process.

Much more still needs to be done to improve the personnel security program. During Fiscal 1982, a select panel was formed at the direction of the Deputy Undersecretary of Defense (Policy) to review the DOD Personnel Security Program. In its report, published in April 1982, the panel made a number of important recommendations for improving the program. In addition, the panel took note of the lack of information available for program evaluation purposes, and the need for research studies and analyses in several areas, including psychological testing to supplement background investigations.

This led to discussions with the Naval Postgraduate School and the initiation of a number of research projects centering on prescreening and psychological testing for high-risk jobs. An important element for the research effort, automated individual personnel records for all Defense components, were available through the Defense Manpower Data Center files maintained at the Naval Postgraduate School.

One of the first steps taken by the Naval Postgraduate School was to bring in a copy of the computerized Defense Central Index of Investigations file (DCII) maintained by the Defense Investigative Service, and to merge it with Defense Manpower Data Center personnel data bases. The DCII would identify Defense personnel receiving background investigations, and the Defense Manpower Data Center files would provide information on their characteristics, performance, and behavior during military service. It would now be possible to identify the kinds of people receiving background investigations, when they received them, what occupations they were in, and how they made out while on active duty. Further, since the Defense Manpower Data Center maintains personnel data bases historically, it would be possible to perform retrospective studies -- to recreate the populations entering the military over the last ten years and more, and to examine the relationships between personnel and investigative actions during that time frame.

The value of combining investigative and personnel data bases for research, program analysis, and auditing purposes can be illustrated by one of the ongoing studies at the Naval Postgraduate School. During the past five years, over 27,000 enlistees receiving background investigations for assignment to sensitive positions were later discharged for reasons of unsuitability, unfitness, or other behavior problems. The 27,000 enlistees represent approximately twenty percent of those servicemen who were discharged in that period of time who had background investigations. The specific reasons for their discharge are shown in attachment 1.

Many of the 27,000 enlistees discharged had received Top Secret and Sensitive Compartmented Information clearances for high-risk jobs. To better understand the high failure rate for this group, background investigation and discharge records will be examined by the Naval Postgraduate School for samples drawn from this population. This study is still underway and specific findings will not be known until further research is completed. However, there are a number of possible explanations: (1) the background investigations lacked accuracy by not identifying unfavorable behavioral patterns for the individuals concerned; (2) unfavorable behavioral patterns were identified but the adjudicative process did not make effective use of the information; and (3) the early behavior patterns for this group were favorable -- their problems arose after background investigations were completed. All three factors are likely to be involved. The real question is to what degree.

Another major research project being conducted at the Naval Postgraduate School is to evaluate the effectiveness of prescreening programs now used by the Services in selecting recruits for high-risk jobs, and to determine the potential of psychological tests for assessment purposes. These studies have become increasingly more feasible with the ability to use investigative and personnel data bases for analysis purposes. Findings from a number of the studies are expected within the next six months.

In addition to the Naval Postgraduate School research program, a large-scale research effort is now being conducted by the Navy Personnel Research and Development Center to develop a special test for DOD-wide use in enlisted selection. This test is based on biographic and related information known to predict military attrition, and will be used to screen out those applicants for service most likely to be discharged for unsuitability. Since individuals who score high on this measure are least likely to be behavioral problems in service, the test should also be useful in evaluating recruits for high-risk jobs. The full implications of using measures of this type will be discussed later on.

While the Naval Postgraduate School has been focusing its research effort primarily on prescreening measures, a far more extensive research effort is required. The problem is that relatively little is known about the quality of all components of the personnel investigation process, and even less, perhaps, about how to apply the information it provides.

While large investments have been made by the Military Services in behavioral science research to evaluate and improve personnel selection, assignment, training, and utilization procedures, there has been little involvement by Defense scientists in the research needed to evaluate and improve personnel security investigations. This is particularly unfortunate since the application of behavioral science and operations research methodologies are particularly relevant here.

There is so much to be done that it is hard to know where to start. There are, however, a number of readily identifiable areas where personnel security research should be particularly productive. These are largely in respect to personnel investigation procedures, and include the following problem areas:

(1) Requirements -- It is important that Defense and Service policies and practices be evaluated that determine who receives a background investigation. There are large Service differences in the number of military personnel requiring background investigations. While this may represent differences in mission, the disparities may also be showing differences in Service policies and practices. Use of Defense-wide surveys, task analysis, and evaluation of available personnel and investigative data should furnish the information needed to evaluate the legitimacy and adequacy of Service requirements for background investigations.

(2) Timing -- We need to know whether or not personnel security investigations are being initiated at a point in time consistent with good personnel management practices. Should background investigations be initiated before, during, or after training for various types of high-risk jobs? And when should reinvestigations be accomplished? While the issues here are complex, the application of systems analysis techniques should lead to more effective use of investigative resources, reduce nonproductive time spent waiting for clearances, and identify the best points in time for "bring-up" investigations.

(3) Coverage -- It is important to identify the types of information needed for an effective behavioral evaluation and to determine if the investigative process provides, or could provide, this information. A panel of behavioral scientists should evaluate the completeness of the current background investigation procedure, and recommend additional coverage where needed.

(4) Procedures -- We need to know the cost-effectiveness of using various information sources and collection techniques in obtaining the data required for personnel assessment purposes. There are experimental techniques available to tell us the relative yield and accuracy of using specific reference and records sources, as well as the most cost-effective media for data collection.

(5) Accuracy -- Though reliable and accurate data are crucial to the assessment process, very little information is available concerning the quality of background investigation procedures. The use of sampling techniques and product evaluation procedures of the type applied in industrial settings should have particular applicability for personnel security investigations.

(6) Validity -- Assessment information has value to the extent that it predicts later behavior. Adjudicators need to know the relationships between background investigation information and subsequent behavior to make effective clearance decisions. Powerful statistical procedures are available for analyzing the validity of background investigation data in predicting important behavioral criteria and in developing composite scores maximally predictive of these criteria.

(7) Utility -- The question to be addressed here is how best to use the products of personnel security investigation procedures. Little is known of the impact of adjudicative decisions on assignment, training, performance, and utilization actions. Operations analysis procedures could help evaluate these impacts and suggests ways to reduce their negative effects.

Research and analysis performed in these areas should lead to a more effective personnel security program by reducing the number of unnecessary investigations now being performed, increasing their quality, and improving the utilization of the information they provide.

I would now like to make some general observations and recommendations concerning the personnel security program. First, it is important to recognize that most of the adverse information developed through background investigations relates to behavioral problems, rather than loyalty. Second, in collecting and adjudicating adverse information, the assumption is being made that individuals with very unfavorable background histories are poor security risks -- people likely to continue having behavioral problems. It is important to note here that, through the application of current adjudicative guidelines and practices, about five percent of those receiving background investigations are denied clearance.

Unfortunately, what the current personnel security process does not take into account is that there are still wide differences in behavioral adjustment history and expected behavior among the ninety-five percent of those cleared for sensitive duties. All to frequently, recruits with a history of preservice adjustment problems receive clearances indistinguishable from those of fellow recruits with exemplary preservice records -- although much more likely to be discharged for unsuitability later on. It is hardly likely that a process which identifies the bottom five percent of those receiving background investigations as behavior risks, and everyone else as equally acceptable, is providing the best candidates available for assignment to high-risk jobs.

I think we should look very carefully at the possibility of selecting people into high-risk jobs rather than selecting them out. For the enlisted population the situation may be analogous in some respects to the use of aptitude scores for recruit assignment purposes. An aptitude battery is now administered to all applicants for military service, and only those with the highest scores are considered for assignment to highly technical positions. We should use the same approach by obtaining personnel assessment information from all recruits, and identifying those with the highest adjustment potential for assignment to high-risk jobs.

I believe that this can be done. Although we would be unable to have background investigations completed for all recruits to identify the most promising among them, there are less costly procedures that could be used for initial selection purposes. The suitability test being developed by the Navy Personnel Research and Development Center and additional self-report behavioral history measures should provide much of the information now obtained through background investigations. Further, the use of automated scoring procedures for these data would provide "adjustment potential" scores predictive of later military behavior. Background investigations could then be accomplished for the most highly qualified recruits to check on the accuracy and completeness of the information obtained through the self-report procedures.

There are many advantages to using this approach. Most important, it would reduce the number of enlistees assigned to high-risk jobs who are later discharged for unsuitability. It would also reduce the number of enlistees denied clearance. Further, for those recruits not initially assigned to high-risk jobs, "adjustment potential" scores would be a matter of record and still usable for later screening purposes. This approach would be quite similar to the current use of aptitude scores for later assignments, and allow for overriding at a later data after individuals have proved themselves.

Eventhough it is possible to improve the personnel security investigation process by taking actions of the type described above, there are still serious limitations to the selection approach. We are faced with the fact that we cannot predict the behavior of individuals with the degree of precision needed. The best that can be done is to identify groups of individuals with somewhat different probabilities of satisfactory behavior. To illustrate this point, based on current screening procedures, groups of recruits can be identified at service entry whose first-term unsuitability discharge rates will vary from about eight percent to over fifty percent. This is a level of accuracy roughly comparable to that of aptitude scores in predicting training success. While the accuracy of suitability screening would be further improved through use of the measures previously described, there would still be significant numbers of later "failures" even in the most highly selected groups. We can reduce the odds of later misbehavior significantly with the use of valid selection procedures -- but in no case can we reduce the odds close to zero.

It is essential, therefore, to have a personnel security system that takes into account the need for continuing observation and periodic evaluation of the people assigned to high-risk jobs. A standardized monitoring and assessment program is needed, with military and civilian supervisors and managers fully responsible for its effective administration. In some respects, the Defense Personnel Reliability Program already uses this type of approach.

To conclude, it is apparent that relatively little is known about the effectiveness of the Defense Department's Personnel Security Program. The large number of unsuitability discharges among those cleared for Top Secret and related duties indicates that there is ample room for improvement of the current program. It is essential that behavioral science and operations analysis techniques be applied in a large-scale research effort to evaluate and refine the personnel security program. The effort is long overdue.

#

ENLISTED PERSONNEL, ALL SERVICES, WHO RECEIVED BACKGROUND INVESTIGATIONS: DISCHARGES FOR FAILURE TO MEET MINIMUM BEHAVIORAL STANDARDS DURING THE PERIOD FY 1980 THROUGH FY 1984

REASONS FOR DISCHARGE	NUMBER	PRECENT OF TOTAL
Unsuitability	12,639	46.4
Expeditious Discharge	4,360	16.0
Trainee Discharge	2,983	10.9
Motivational Problems	2,691	9.9
Unsuitability	2,605	9.6
Character or Behavior Disorders	7,922	29.1
Drugs	4,127	15.2
Character or Behavior Disorders	1,908	7.0
Homosexuality	1,151	4.2
Alcoholism	642	2.4
Sexual Perversion	94	.3
Offenses	5,978	21.9
Discreditable Incidents	2,755	10.1
Misconduct, Disciplinary Infractions	1,632	6.0
Court Martial	1,146	4.2
Civil Court Conviction	389	1.4
AWOL, Desertion	56	.2
Other	695	2.6
Fraudulent Entry	430	1.6
Financial Irresponsibility	196	.7
Inaptitude	45	.2
Security	24	.1
Total	27,234	100.0

DEVELOPMENT AND OPERATION OF A PERSONNEL SECURITY RESEARCH PROGRAM TO SUPPORT DEFENSE REQUIREMENTS

Federal agencies have developed large-scale personnel research programs to evaluate and improve personnel selection, assignment, training, and related personnel procedures. There has been relatively little research conducted by behavioral scientists, however, to evaluate and improve personnel security screening procedures. This has had an adverse effect on personnel security programs, since the application of behavioral science and operations research methods and procedures are particularly relevant to the personnel security area.

There is now evidence that large numbers of enlisted personnel assigned to sensitive duties are being discharged for reasons of unsuitability. This raises serious questions concerning the adequacy of current personnel security screening procedures.

To address this and related problems, the Department of Defense is making plans to develop and conduct a large-scale personnel security research program. The plan for a DoD-wide program calls for research in a number of areas relevant to both personnel security screening and continuing evaluation procedures. Major research areas are described below:

(1) Requirements -- It is important that Defense and Service policies and practices be evaluated that determine who receives a background investigation and who requires continuing evaluation. There are large Service differences in the number of military personnel needing background investigations. While this may represent differences in mission, the disparities may also be showing differences in Service policies and practices. Use of Defense-wide surveys, task analysis, and evaluation of available personnel and investigative data should furnish the information needed to evaluate the legitimacy and adequacy of Service requirements for background investigations and continuing evaluations.

(2) Timing -- We need to know whether or not personnel security investigations are being initiated at a point in time consistent with good personnel management

practices. Should background investigations be initiated before, during, or after training for various types of high-risk jobs? And when should reinvestigations be accomplished? While the issues here are complex, the application of systems analysis techniques should lead to more effective use of investigative resources, reduce nonproductive time spent waiting for clearances, and identify the best points in time for "bring-up" investigations.

(3) Coverage -- It is important to identify the types of information needed for effective personnel security assessments and to determine if the investigative process provides, or could provide, this information. A panel of behavioral scientists should assess the completeness of current background investigation and continuing evaluation procedures and recommend additional coverage where needed.

(4) Procedures -- We need to know the cost-effectiveness of using various information sources and collection techniques in obtaining the data required for personnel assessment purposes. There are experimental techniques available to tell us the relative yield and accuracy of using specific reference and records sources, as well as the most cost-effective media for data collection.

(5) Accuracy -- Though reliable and accurate data are crucial to the assessment process, very little information is available concerning the quality of background investigation and continuing evaluation procedures. The use of sampling techniques and product evaluation procedures of the type applied in industrial settings should have particular applicability for here.

(6) Validity -- Assessment information has value to the extent that it predicts later behavior. Adjudicators need to know the relationships between assessment information and subsequent behavior to make effective clearance decisions. Powerful statistical procedures are available for analyzing the validity of assessment data in predicting important behavioral criteria and in developing composite scores maximally predictive of these criteria.

(7) Utility -- The question to be addressed here is how best to use the products of personnel security assessment procedures. Little is known of the impact of adjudicative decisions on personnel assignment, training, performance, and utilization actions. Operations analysis procedures will help evaluate these impacts and suggest ways to reduce their negative effect.

A DoD Personnel Security Research Program should be established at the earliest possible date to initiate research in the above areas, and on a priority basis. Personnel security research initiatives being accomplished through the Naval Postgraduate School and the Navy Personnel Research and Development Center have already shown the desirability of this course of action.

DoD Personnel Security Research Program

- Increasing evidence that Defense's personnel security program not effective
- Behavioral science and operations research program needed to evaluate and improve personnel security procedures
- Defense has capability to develop and sustain its own personnel security research program
    - -- availability of qualified personnel researchers
    - -- availability of automated investigative and personnel data bases
    - -- availability of computer resources for large scale cross-sectional and longitudinal analyses
- Defense personnel security research program can also serve as core activity for interagency research effort
    - -- assist in designing and conducting research for other federal agencies on a reimbursable basis
- The Naval Postgraduate School and the Navy Personnel Research and Development Center are now accomplishing a number of personnel security research initiatives.
- These organizations should jointly develop and sustain a Defense-wide personnel security research program.
- Defense needs to identify funding source for a continuing program.

Senator **Nunn**. Tomorrow morning, we will begin in this room at 9:30. We will first hear Mr. Thomas O'Brien, Director of Defense Investigative Service. Then we will have special witness Christopher J. Boyce, followed by a panel of industrial witnesses. Then we will wrap up the hearings with Gen. Richard Stilwell, Deputy Under Secretary of Defense, and he will be accompanied by Britt Snider, Director of Counterintelligence Security Policy for the Department of Defense.

So we will convene these hearings again tomorrow morning. Again, let me thank our witnesses for being here. Thank you.

[Senators present at the recess: Senators Nunn and Gore.]

[Whereupon, at 11:55 a.m., the subcommittee recessed to reconvene at 9:30 a.m., Thursday, April 18, 1985.]

FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

THURSDAY, APRIL 18, 1985

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The subcommittee met at 9:35 a.m., in room SD-342, Dirksen Senate Office Building, under authority of S. Res. 85, section 13, dated Feb. 28, 1985, Hon. William S. Cohen, presiding.

Members of the subcommittee present: Senator William S. Cohen, Republican, Maine; Senator Sam Nunn, Democrat, Georgia; Senator Lawton Chiles, Democrat, Florida; and Albert Gore, Democrat, Tennessee.

Members of the professional staff present: Daniel F. Rinzel, chief counsel; Nicholas Chiarkas, deputy chief counsel; Eleanore J. Hill, chief counsel to the minority; Katherine C. Bidden, chief clerk; John F. Sopko, assistant counsel to the minority; David Glendinning, staff counsel; Leonard A. Willis, Glenn W. Fry, and Fred Asselin, investigators for the minority; Sarah Presgrave, executive assistant to the chief counsel; Kathleen A. Dias, executive secretary to the chief counsel to the minority; Mary Robertson, assistant chief clerk to the minority; and Townsend Feehan, receptionist.

[Senators present at the convening of the hearing: Senators Cohen and Nunn.]

OPENING STATEMENT OF SENATOR COHEN

Senator COHEN. The committee will come to order.

This morning, the Permanent Subcommittee on Investigations convenes its third day of hearings to evaluate the Federal Government's personnel security clearance programs. During the past 2 days, the subcommittee has received testimony from Government and industry witnesses who have identified several significant problems with the present system, including the following: proliferation of clearance requests; scarcity of investigative resources to handle the increasing workload; inconsistency between agency procedures for conducting background investigations and granting clearances; absence of field investigations for, or periodic review of, secret clearances which constitute the largest category of industrial clearances; and reluctance by agencies to deny or revoke clearances except in the most flagrant cases.

These problems, among others, have resulted in several publicized espionage cases which will be discussed at today's hearings.

Perhaps the most well-known case involves Christopher Boyce, who was working for TRW and was convicted and sentenced for selling classified documents to the Soviets.

The two other cases involve William Holden Bell, a former Hughes Aircraft employee and James Harper and his accomplice, Ruby Schuler, formerly employed by Systems Control Technology. These individuals were convicted of selling classified information to Polish agents.

We hope the testimony on these cases will help us to identify and remedy the flaws in the security clearance process.

At this point, I would like to commend Senator Nunn for his leadership in these important hearings and yield to him for any opening comments he cares to make.

Senator NUNN. Thank you, Mr. Chairman. I made mine a couple of days ago. So we will just proceed here. Thank you very much for your comments and for your interest in these hearings. I think we have had a good set of hearings so far. Without any doubt, we have identified several deficient areas in our personnel security procedures in the Government. We have also, I think, identified pretty explicitly some of the delays and problems in both looking at changes in the law and in the regulations.

We have had an ongoing process with a task force looking at this now for a couple of years. The National Security Council has had a recommended set of options from that task force for revamping this whole procedure for over a year, and we have not seen anything.

I notice, Mr. Chairman, in this morning's Washington Post a story entitled, "Government Is Drafting Electronic Security Rules," and while I applaud that, it seems that we are doing a great deal in the computer area, but we are lagging way behind in the personnel area.

[The article referred to was marked "Exhibit No. 18," and follows:]

EXHIBIT NO. 18

[From the Washington Post, Apr. 18, 1985]

GOVERNMENT IS DRAFTING ELECTRONIC SECURITY RULES

(By Michael Schrage)

The Reagan administration is drafting guidelines to classify all national security-related information throughout the federal government—including civilian agencies—as part of an effort to increase computer and telecommunications security.

Much of the information now in government computers is not protected and is widely available. A special national security committee will decide how much of that information needs protection and how that protection should be fashioned.

"We are going to be issuing guidelines for protecting sensitive information for every federal system," said Donald C. Latham, assistant secretary of Defense for communications, command and control. "Every system will require some level of access control."

Latham is chairman of the eight-month-old interagency National Telecommunications and Information Systems Security Committee (NTISSC) that was established to devise policy on electronic security for the government.

This new push for information security also propels the top-secret National Security Agency, the country's largest intelligence organization, into a major role as the nation's arbiter of security technology standards for civilian agency systems as well as military uses.

The guidelines, which will be released over the next few months, promise to rekindle debate over the extent of classification as well as how best to protect sensitive data. The Reagan administration has been vigorous in bringing many different kinds of information under a security umbrella.

"It's very difficult to define classified information," said Robert Conley, deputy assistant Treasury secretary for advanced technology and analysis and a member of the security committee. "There's basically three categories of information: national security, public domain, and sensitive. Sensitive information falls between national security and public domain—it's defined by omission.

"Now you have to decide by what mechanism you want to protect that information," he said.

As the federal government relies on computer networks and ordinary telephone conversations to conduct even the most sensitive business, traditional methods of classification for paper files and documents are seen as no longer adequate.

The fact that computer and telecommunications technologies can be breached by electronic intercept and entry has prompted the decision to launch a set of security countermeasures in both classification and technology.

One result could be that sensitive information now stored in civilian agency computers would fall under a new national security classification. For example, the guidelines may require the Commerce Department to store information on export licenses of high-technology items in a more secure computer system, or insist that certain defense contractors install new procedures to deny unauthorized computer access to their data.

Presumably, implementing the new guidelines would prevent the recurrence of such episodes as the one in which Milwaukee teen-aged computer hackers used their home computers to tap into the files of a Los Alamos National Laboratory computer more than a year ago.

This new emphasis on electronic security policy springs from National Security Decision Directive 145, signed by Reagan last fall, which identified Soviet electronic eavesdropping—particularly on phone calls—as a national security threat. It called for a comprehensive approach to protecting both telephone and computer communications.

The most publicized aspect of NSDD 145 has been the announcement that the government plans to procure half a million "secure" phones that scramble conversations.

These computer and communications security initiatives—which most experts estimate would cost billions of dollars to implement—give important new powers to the NSA. The NSA, which designs the nation's military codes, will become an electronic security research and development arm, a security standards setter and the agency that transfers security technology into both the federal government and private industry.

An NSA spokesman said the directive and the committee "broadens both the communications and computer security missions of this agency. We will be establishing trusted computer standards that can be met for federal agencies . . . and the private sector."

These standards are being developed by NSA's recently established National Computer Security Standards Center. In the past, other national security directives gave the Commerce Department jurisdiction over nonmilitary computer security standards.

Computer and communications security has historically been a low-priority item for nonmilitary agencies, according to Sanford Sherzen, an information security consultant who recently completed a report on the topic for the Office of Technology Assessment. "It's been almost nonexistent . . . almost a leaderless area," he said.

The White House Office of Management and Budget has stated that it does not want the cost of security to be a special item on the budget when agencies procure data-processing equipment, so there is likely to be a conflict between the level of security that NTISSC requires and the money that OMB is willing to fund for it.

Assessing the ultimate cost of the new security measures is impossible, because nobody knows how many computer systems there are in the government, according to Latham. NTISSC has issued a "data call" throughout the government to find out.

[At this point in the hearing, Senator Gore entered the hearing room.]

Senator NUNN. That is a considerable concern. According to all the expert testimony, the biggest problems we have in security relate to human beings, and that is a gigantic problem.

Mr. Chairman, I have said this before, but I think it is important to emphasize the scope of the problem involves the number. I don't know whether there is any way to reduce dramatically the numbers involved in security clearances or not. When you have 4.2 million people cleared in this country—4.2 million—cleared for classified information, no matter how you organize the governmental apparatus—DIS, the Office of Personnel Management, and the others—it is a staggering problem.

I will have more to say on that later. But I do believe it is time for the legislative branch to take a very careful look at this. We appreciate the witness this morning from the Defense Investigative Service. We look forward to that testimony. We also look forward to the testimony of Christopher Boyce. I think that will be enlightening in terms of someone who has actually been engaged in and convicted of espionage telling us from his own perspective some of the interesting observations he has about our own systems of protection.

We also have the industrial witnesses this morning from various companies that have dealt with this problem, as you have already outlined. I think we will be interested in hearing about three particular cases where we have had very severe security breaches. For those of you in the audience, at some time in the next several weeks, we will certainly be having some specific legislative and regulatory recommendations.

Senator COHEN. Our first witness this morning is Thomas O'Brien who is Director of the Defense Investigative Service which is responsible for conducting all personnel security investigations for the Department of Defense.

Mr. O'Brien, in the interest of time, I hope you can perhaps summarize your prepared testimony, and the full statement will be included in the record.

Before you begin testifying, would you stand and raise your right hand?

Do you swear the testimony you will give before the subcommittee will be the truth, the whole truth and nothing but the truth, so help you God?

Mr. O'BRIEN. I do.

Senator COHEN. Mr. O'Brien.

TESTIMONY OF THOMAS J. O'BRIEN, DIRECTOR, DEFENSE INVESTIGATIVE SERVICE, DEPARTMENT OF DEFENSE

Mr. O'BRIEN. Mr. Chairman, I am pleased to have the opportunity to discuss the mission of the Defense Investigative Service with this committee.

I will summarize my statement and provide just a short statement here, and I ask that my entire statement be submitted for the record.

The Defense Investigative Service is designated by the Department of Defense as a criminal justice, personnel security investigative and industrial security agency. We report to the Deputy Under Secretary of Defense for Policy. We are responsible for conducting all personnel security investigations for the Department of Defense. These investigations are necessary to determine eligibility for security clearances, and they involve military, civilian and industrial personnel.

This year, we will conduct approximately 220,000 such investigations and, in addition, we will complete over 900,000 national agency checks.

Our second major mission is the administration of industrial security. The Defense Industrial Security Program provides the framework for ensuring that classified information entrusted to industry is property safeguarded. This program involves not only DOD contractors, but contractors of 18 other departments and agencies of Government. There are today over 14,000 cleared contractor facilities employing about 1.4 million cleared people in industry.

DIS was established in 1972. Prior to that time, personnel security investigations were conducted by the Army Intelligence Command, Naval Investigative Service, and the Air Force Office of Special Investigations. The consolidation was responsible for significant savings. Although our workload has increased by over 52 percent between 1973 and 1985, the total human resources applied to the mission were reduced during the same period by almost 7 percent, as reflected on this chart over to my right.

In 1980, the Industrial Security Program was transferred to DIS from the Defense Logistics Agency. DIS is an entirely civilian organization. We are authorized 3,693 people. Our budget for fiscal year 1985 is $117 million.

Because of reduced resources and a significant increase in requests for investigations, especially for contractor personnel, in April 1981, we found ourselves with a pending caseload of over 84,000 cases and completion times for background investigations were averaging over 190 days. In May 1981, DOD put a moratorium on periodic reinvestigations and DIS was given 668 additional spaces. These actions contributed significantly to reducing our backlog and completion times. By the end of 1983, the backlog was down to 36,000 cases and completion times were averaging about 70 days. Both of these numbers started to increase during 1984 due to a significant increase in the number of requests and because of the start up of periodic reinvestigations and the enhancement of our interview-oriented background investigation.

Our pending caseload during the second quarter of fiscal year 1985 was about 56,000 cases and completion times are averaging about 92 days overall and 85 days for cases in which there are no overseas leads. Because of this increased workload, the President's budget for fiscal year 1985 provided a strength of some 320 spaces above that authorized for 1984. Some of these increases in personnel resources are for the Industrial Security Program which, as I will point out later in my statement, is also experiencing significant growth.

During 1984, DIS completed about 195,000 investigations. This figure is significantly higher than prior years. For example, in 1980, we completed only 143,000 cases. As impressive as this increase in production has been, it fell short by some 12,000 cases of completing the 270,000 investigations that were requested in 1984.

For this fiscal year, we are projecting 219,000 requests for investigations. However, we have recently decided to defer some periodic reinvestigations to prevent case openings from exceeding closings during this fiscal year.

To give you an idea of how we stand in relation to other Federal Government organizations, which also conduct personnel security investigations, the Office of Personnel Management, which is the next largest, conducts only about 20 percent of the number of investigations that DIS conducts. We have initiated several major programs to enhance quality and security. In 1981, we introduced the interview-oriented background investigation. This was the first significant change since World War II in the way personnel security investigations are conducted. We call these IBI's. It involves an indepth interview of the subject, and we have found this to be a very productive source. We also, of course, conduct additional leads in each of these investigations.

The second major enhancement of security occurred in 1983 when DOD began a new program of periodic reinvestigations, not only with persons with access to Sensitive Compartmented Information, but for those people with top secret clearances as well.

Formerly, periodic reinvestigations had been only for people with SCI access, and they consisted of simply a check of certain national agencies. The scope of the new periodic reinvestigation includes a subject interview. The program is designed to identify those cleared people who may no longer be reliable or trustworthy.

I should point out that in most all instances of espionage involving cleared people, their involvement with foreign intelligence developed subsequent to their initial investigation and clearance. This new and aggressive periodic reinvestigation program should serve as a deterrent to those who might otherwise become traitors.

In an organization as large as the Department of Defense, there is always the danger that more investigations will be requested than are absolutely necessary. DOD has done a number of things to prevent unnecessary requests for investigations. Just recently, the Office of the Secretary of Defense has proposed a quota system and we're working closely with OSD in this effort. We are quite optimistic that a system of controls will be put into effect in the near future.

One of the major problems in conducting personnel security investigations is the difficulty we are encountering in attempting to obtain access to local criminal justice records. In recent years, some jurisdictions have curtailed access to convictions and, in other jurisdictions, we are getting no criminal justice information whatsoever. Historically, criminal records have been one of the better sources of investigative information. To appoint an individual to a sensitive position involving nuclear weapons aboard a submarine or to provide an individual sensitive compartmented information without knowing that individual's prior arrest record represents a significant security vulnerability.

DIS is working with each jurisdiction where problems are encountered. In some cases, we have had success, and in other jurisdictions, we continue to have to close investigations without having access to this vital information. I consider this to be one of our most crucial problems, and I feel that a concerted effort at the national level is necessary in order to bring State and local jurisdictions into a position of support of our overall national security priorities.

Senator NUNN. Mr. Chairman, would you permit a question at that point? On that subject, we have heard over and over again that State and local governments are not cooperating in supplying criminal records. Is that because of the Federal Privacy Act? Is that because of the relationship between agencies? What is the reason?

Mr. O'BRIEN. I think there are a variety of reasons. Now, let me make the record straight, most jurisdictions provide us the information, but there are some significant jurisdictions that do not. And in each State or local jurisdiction, there is a particular problem. They are not all the same.

For example, in Washington, DC, we get conviction information only if it's within the last 10 years. There are a lot of people who are arrested in the District of Columbia but for whatever reason are not convicted. We don't get that. It is particularly significant because DC does not provide arrest data to the Federal Bureau of Investigation either. So when we do our National Agency Check, we don't get that.

In the State of California, it's the Fair Labor Standards Act of California which has language in it that has been interpreted locally to preclude us access in California. We do get access in some locales in California, but the State policy precludes it.

I personally have been to Sacramento attempting to get the legislation changed in California, but to date we have not been successful.

Senator COHEN. Isn't California the State where you have perhaps the largest concentration of defense-oriented industries?

Mr. O'BRIEN. Yes, sir; it is.

Senator COHEN. Wouldn't it behoove this Government at least to indicate that fewer security clearances are going to be granted to those institutions and have the major contractors put pressure on the State legislature to say we are going to lose the business if you don't change the law?

Mr. O'BRIEN. We have been attempting to do this. We have been trying to get a member of the California legislature to sponsor legislation, but to date we have not been successful.

Senator COHEN. What I am suggesting, it is not going to happen unless there is direct economic pressure.

Mr. O'BRIEN. I agree.

Senator COHEN. But a legislator introducing a bill is not going to produce a change in the law unless there is some serious consequence involved.

Mr. O'BRIEN. Yes, sir.

Senator NUNN. Have you submitted any proposed Federal legislation from the Defense Department or executive branch to deal with this problem? Have you any recommendations?

Mr. O'BRIEN. Yes; we have submitted legislation. I don't have it here however.

Senator NUNN. As an administration proposal or is that just from Defense within the administration?

Mr. O'BRIEN. I have to double check exactly. We drafted some——

Senator NUNN [interposing]. Whatever the status of it, could you furnish it to us for the record?

Mr. O'BRIEN. I certainly will.

Senator NUNN. Thank you.

[The legislation referred to follows:]

A BILL

To allow designated Federal investigative agencies, when conducting investigations for the purpose of determining qualifications or suitability for Federal employment or trustworthiness for clearance for access to classified or specially restricted information or material, to have access to certain records and information that may otherwise be unavailable.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Investigative Access Control Act of 1982".

Sec. 1. (a) Records, materials, and information necessary for conducting an investigation for the purpose of determining an individual's qualifications or suitability for Federal employment, or trustworthiness for clearance for access to classified or specially restricted information or material includes the following:

(1) Criminal history records and information pertaining to the individual consisting of identifiable descriptions and notations of arrests, detentions, indictment, informations, or other formal criminal charges, and any dispositions arising therefrom, shall be provided by criminal justice agencies.

(2) Personal or employment records and information shall be provided by employees and former employers of such individuals.

(3) Financial and credit records and information pertaining to the individual shall be provided by financial and credit agencies and institutions.

(4) Records and information relating to the education of an individual shall be provided by the educational institution.

(b) Release of records, information, and material pursuant to subsection (a) shall be provided by criminal justice agencies, as defined by Title 28 CFR 20.3(c) and shall include both State and local agencies, to Federal investigative agencies as defined in section 2.

(c) Subsection (a) shall apply notwithstanding any provision to the contrary contained in the Right to Financial Privacy Act of 1978, the Family Educational Rights and Privacy Act, Sections 4424 and 6103 of The Internal Revenue Code of 1954, and law or regulation of any State or of any locality within a State, and any other law of the United States.

Sec. 2. For purposes of this Act:

(1) The term "Federal investigative agency" means--

(A) the Central Intelligence Agency;

(B) the Federal Bureau of Investigation and other investigative elements of the Department of Justice;

(C) the U.S. Office of Personnel Management;

(D) the U.S. Postal Service; and

(E) the investigative elements of the Department of Defense, Department of State and the Department of Treasury

(2) The term "qualifications" means the capacity or ability of the person investigated to perform satisfactorily the duties of the position in the Government for which the person is being considered or to which the person has been appointed.

(3) The term "suitability" means a requirement or requirements for employment by the Government having reference to the character, reputation, reliability, honesty, trustworthiness, loyalty and other attributes having a bearing on the employment fitness of the person under consideration.

(4) The terms "classified or specially restricted information or material" mean information or material designated pursuant to the provisions of a statute or Executive order or a regulation or order issued pursuant to a statute or Executive order or other authority as requiring a specific degree of protection against unauthorized disclosure for reasons of national security or other authorized purpose.

(5) The term "State" means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, Guam, the Virgin Islands, American Samoa, the Trust Territory of the Pacific Islands, and any other territory or possession of the United States.

(6) The terms "local" and "locality" mean any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal or other local government level.

Sec. 4. This Act shall become effective with respect to any investigation conducted by a Federal investigative agency for any of the purposes specified in section 1 which begins after the date of the enactment of this Act.

Mr. O'Brien. Let me turn to our second major mission, the Defense Industrial Security Program. Here, again, we have also seen an explosion in the number of clearances requested. This results primarily from the defense buildup to include the acquisition of sophisticated high-technology weapons and, to a lesser extent, the current emphasis on contracting out.

The Industrial Security Program is very complex. It involves the safeguarding of classified information entrusted to industry. We have seen the number of cleared facilities in the program grow by over 3,000 in the past 4 months. The impact of this has been dramatic. Inspections of cleared contractors are required every 6 months for those facilities with top secret and secret material, and every 9 months for other facilities.

In 1985, this will necessitate over 22,400 inspections. Not only is the inspection requirement up, but the complexity is also up because of such things as increased use of ADP. For example, the number of ADP systems on which classified information is being processed has increased by over 129 percent since 1982.

Another complexity in the administration of industrial security is the dramatic increase in the amount of foreign investment in that segment of U.S. industry engaged in classified work. This is evidenced by a 33 percent increase in the number of facilities subjected to formal foreign ownership, control or influence determinations. We have a general policy in DOD that a company that is under foreign ownership, control, or influence is not eligible for a security clearance. However, in some cases, it requires considerable analysis before a decision can be made.

To conclude, I would like to point out that in security, we are constantly reassessing and improving our priorities to strike the proper balance. It is a difficult and delicate balance. First and foremost, we must fully assess and counteract the threat from our adversaries. We must also operate within the bounds of available resources. We must be conscious of the need to minimize security's adverse impact on productivity in industry. Finally, we must be ever mindful of the inherent problems of security in a free society and particularly in the private sector of a free society. It is within these parameters that conflicting priorities must be assessed in order to strike that proper security balance.

Personnel and industrial security is in a way like life insurance. How much do we need, and how much can we afford? However, unlike life insurance wherein clear-cut events will eventually occur which prove the worth of the policy, it is not so simple in personnel and industrial security to know how well one's program is working. That is to say whether or not we've taken out sufficient insurance.

That completes my formal statement. I will be happy to respond to your questions.

Senator Cohen. Thank you very much, Mr. O'Brien. I think we all share the belief that there is no perfect way to construct a leakproof clearance system. But because we can't do everything doesn't mean we shouldn't do something, and something is what we are going to be struggling to come up with in the way of positive recommendations and change.

You indicated in your opening testimony the need for a quota system. What else? And if you have simply a quota system and shrink the number of clearances, how does that relate to maintaining effectiveness and efficiency within the defense industry itself?

Mr. O'BRIEN. I should point out, of course, with the administration's buildup in defense, we're bound to have in these high-technology areas increasing requests for clearances. I think we have to take that as a given. Now, in 1983, when we started this periodic reinvestigation program, for the first time in the Department of Defense, we did establish a quota system with respect to these periodic reinvestigations, and so that's enabled us to control our input somewhat.

Now, requests for initial investigations have been going up dramatically. Just within the last 2 months or so, we've been working with the Office of the Secretary of Defense with a view toward establishing a quota system overall which would apply to the military departments and to contractors so that they would be limited—particularly in the numbers of top secret clearances requested, because this is where the heavy investigative effort is concentrated.

Senator COHEN. You mentioned before that there are problems in the District of Columbia and California. What about Massachusetts or Virginia?

Mr. O'BRIEN. Well, Massachusetts, in 1972, cut us off entirely, and we went about 10 years without criminal history record information in that State. I went to Massachusetts and met with State officials and we worked it out. Now we are getting access very well in Massachusetts.

In Virginia, the problem is a little different. Virginia has a central index of arrests they maintain in Richmond, and they charge, I believe it's $5 per check. And the policy of the Department of Defense is not to routinely pay for these because if all jurisdictions required payment, it would be a horrendous expense.

Now, most jurisdictions in Virginia let us conduct checks locally, but there are a few places such as Hampton Roads where we are not getting full access at the present time. We keep working with local officials, and as soon as we get one fixed another problem breaks out.

Senator COHEN. OPM and DIS apparently have some different standards. You are responsible for conducting the major number of security investigations. Is there a different standard for someone who works in the Commerce Department than DOD, even though they might have access to the same classified information?

Mr. O'BRIEN. Well, the standard for civilian employees in Government is set forth in Executive Order 10450. We conduct, for civilian employees of the Federal Government who have access to top secret or are in critical sensitive positions a standard background investigation, a 5-year scope, and it's the same investigation we have been doing for many years.

Now, in 1981, when we introduced this new interview-oriented background investigation, we initially were going to use this new concept on civilians as we are using them on military and industrial. But OPM objected. They have an oversight role for Executive Order 10450. So we went back to the traditional background investigation.

Senator COHEN. Do you think you should change that?

Mr. O'BRIEN. Yes; in my view, the IBI is a more effective investigation, and I think it should be changed.

Senator COHEN. What about military, civilian, and industrial employees? Are they given the same background checks for secret and top secret clearances?

Mr. O'BRIEN. Yes. Now, for military, industrial and DOD civilians who have access to SCI, we do a special background investigation. That is prescribed by the Director of the Central Intelligence. For DOD industrial and military who have access to top secret, we do our IBI. In our view, the IBI is the most effective background investigation today, and we have recommended, as have a number of others, that we have a single scope to include investigation of those with access to sensitive compartmented information.

Senator COHEN. A number of the more noteworthy espionage cases involved breaches of security by those who had secret clearances only. The question becomes why do you only conduct record checks and limited written inquiries for something as important as that?

Mr. O'BRIEN. We do for secret clearance conduct a national agency check. The problem is basically economic. We just don't have the resources; we don't anywhere near approach the resources that would be required to do a more extensive investigation of people with access to secret. A national agency check is a pretty good check. It screens out people who have been arrested. It comes to the attention of the Federal agencies. The scope of a national agency check.

Senator NUNN. Isn't that just arrest at the Federal level unless the States cooperate? Do you have that all in a central arrest file with the FBI?

Mr. O'BRIEN. Yes; the FBI gets fingerprints of people that have been arrested in local jurisdictions, and most jurisdictions do contribute that. It is quite a comprehensive record of people who have been arrested. In addition to that we tailor the national agency check. If, for example, a person had a former military service, we check that person's military record. If a person has traveled extensively abroad, we check with State and CIA. It depends on what the person has done which will dictate the checks we make.

Senator COHEN. You mentioned before economics is precluding you from doing it. What about the situation where you had the downgrading of the Quincy Shipyard and General Dynamics? It was downgraded from top secret to secret in order to accommodate Mr. Veliotis.

Mr. O'BRIEN. Prior to 1972, the Department of Defense policy was to grant immigrant aliens access through top secret. In 1972, before Veliotis came on the scene, DOD changed its policy so at that time, we would not clear immigrant aliens above the secret level.

When Veliotis was first proposed for that management position at Quincy, we knew that we couldn't continue the facility clearance at the top secret level, so the facility clearance was downgraded to accommodate the highest clearance that could be given to Veliotis as an immigrant alien.

Initially, he wasn't even an immigrant alien. We didn't clear him until after he was legally admitted for permanent residence. For immigrant aliens, we conduct a background investigation. In 1981, the Department of Defense changed its policy further where we don't clear immigrant aliens at any level as a general rule. We have an exception to that rule so that an immigrant alien who has extraordinarly talents that are really needed, may be cleared, but no higher than secret.

At the present time in industry, we are only clearing about three immigrant aliens per month.

Senator COHEN. Well, Mr. Veliotis, to my understanding was allowed to operate the Quincy Shipyard for a period of 12 months without any clearance.

Mr. O'BRIEN. Yes, sir; that's correct.

Senator COHEN. How did that occur?

Mr. O'BRIEN. In our Industrial Security Program, when a new manager comes in, we have a general rule that managers, people who occupy those top management positions must be cleared as part of the facility clearance. In these 14,000 cleared facilities, we have a turnover of top managers which just occurs in the normal course of business. We don't shut a company down while we are getting these executives a clearance. We have provisions to exclude those people from access to classified information. If the company agrees to exclude the person until the clearance is issued, then we permit the facility clearance to continue.

Senator COHEN. You are saying that Mr. Veliotis, as general manager of General Dynamics for a 12-month period, had no access to the classified information?

Mr. O'BRIEN. Yes, sir. At Quincy, there was very little classified work being done. Most of the work being done at the Quincy Yard was on an unclassified basis. The company placed into effect exclusion procedures to preclude his access to classified information. These procedures were accepted by the DLA cognizant security office in Boston and by the Navy.

Senator COHEN. Why did they decide to downgrade it from top secret to secret?

Mr. O'BRIEN. We knew because of the policy, Veliotis as an immigrant alien could not qualify for a top secret clearance.

Senator COHEN. Exactly. What I am suggesting is, you changed the policy to accommodate a general manager, whether or not Quincy was engaged in classified work. You changed the grading from top secret to secret because Veliotis couldn't qualify.

Mr. O'BRIEN. But the net result of that was they could not have access to anything top secret.

Senator COHEN. Only to secret.

Mr. O'BRIEN. Yes, sir.

Senator COHEN. Veliotis, even though he was given no clearance, had access to secret information.

Mr. O'BRIEN. No, sir; we have no evidence that he did, and the exclusion procedures were put into effect to preclude that. We send inspectors in to make sure that doesn't happen. Now I can't guarantee he didn't have access to secret while he was there, but there is no evidence he did. Our procedures are set up pretty tight to preclude that sort of thing from happening.

Senator COHEN. Senator Nunn?

Senator NUNN. Mr. Chairman, following up on that point on the Veliotis case, our staff indicated, as best they can ascertain since they didn't get very much help in this case from the FBI on the Veliotis case, but other agencies did cooperate, that there has been no damage assessment of the Veliotis case from a national security point of view. I am not saying that the fraud part of it has not been investigated, but from a national security point of view, there has been no damage assessment by our Federal Government, at least as far as they can tell.

They further state that the condition preceding any damage assessment, a thorough check of whether he indeed even retrospectively was a national security risk, has not been made.

Is that accurate, or can you shed light on that?

Mr. O'BRIEN. As far as I know, there has not been a damage assessment and I think the reason is we have no evidence Veliotis has been engaged in espionage.

Senator NUNN. You never even checked his background yet. You are not going to have any evidence he was engaged in espionage without a check. I'm not saying he was.

Mr. O'BRIEN. Right.

Senator NUNN. The indications are that he probably, perhaps—probably—may not have been. Nevertheless, it seems to me that in this kind of case when we know the original security checks were woefully inadequate, there would be a backing up and starting over in this matter to see, if, indeed, they knew it could happen.

Mr. O'BRIEN. He has been investigated by the FBI under the indictment. I have not seen that or been involved directly in that. I have to assume that the FBI did a rather thorough investigation that led to the indictment. If there were any indications of espionage, that would have been covered as well.

Senator NUNN. Perhaps. I would be comforted if I thought that was true. We have not received any information like that.

Mr. O'BRIEN. I would suggest you obtain that sort of thing from the FBI.

Senator NUNN. We have tried without success.

Mr. O'BRIEN. They have jurisdiction, so we are really not in that right now. I don't want to cop out on it. It is their jurisdictional area.

Senator NUNN. But damage assessment would be your area, would it not?

Mr. O'BRIEN. No; the damage assessment is done by the procuring activity whose information has been compromised. DIS is responsible for determining if a compromise has occurred and then notifying the appropriate procurement activity. The actual damage assessment is done by the procuring activity whose information would have been lost.

Senator NUNN. One other question on that point. I understand that for a period of time when Mr. Veliotis was head of the shipyard there he was not cleared and that the guards, and so forth, were instructed that he would not have access to certain areas. Do you really think, considering human nature, that the head of a shipyard who hires and fires people and who can set their pay levels, and so forth, can be kept out of certain classified areas by the people he supervises, the people he hires, the people he fires, and the people whose pay he sets?

Mr. O'Brien. I would agree with your point, but this is an area where we have to balance the equities.

Senator Cohen. Excuse me, it is not a question of balancing equities. What you have is a shipyard hiring a manager altering established policy. You ended up downgrading a facility from top secret to secret to accommodate the contractor who hired a general manager who didn't have the clearances and couldn't get them at that level.

So it is not a matter of equities involved. It is a matter of who is running the show.

Mr. O'Brien. Of course, the company decides—the Department of Defense doesn't say who to hire.

Senator Cohen. That is right, but the company should not decide what the policy of the United States is going to be.

Mr. O'Brien. Our policy is that we don't give them a top secret clearance. They elected to go with management that can only be cleared to secret. We said, well, if that is what you decide to do in this location, you will not work on anything top secret, and my understanding is they were not working at the top secret level there anyway. At that time, Quincy was not involved in high-tech or highly classified information.

Senator Nunn. He was also vice president of the company.

Mr. O'Brien. That was later on.

Senator Nunn. After he had been cleared.

Mr. O'Brien. It was my understanding he did not assume a corporate role until after.

Senator 4unn. I understand he was a corporate vice president.

Mr. O'Brien. Only later, after he had been granted a clearance.

Senator Nunn. And consideration was given to downgrading the whole General Dynamics Corp., but that was not done for some reason. Even though Senator Cohen has pointed out the problem relating to the shipyard itself, there is a bigger problem when he is involved in the corporate management and the corporation itself has classified access to everything.

Mr. O'Brien. But we also have a policy that is in effect today whereby we clear a minimum number of officers, owners, and executive personnel that comprise the top management echelon. There may be other people who have the title of vice president for instance, that because of their particular effort, can be excluded, and we require the company to execute exclusion provisions as a matter of record in the board of director minutes to exclude these people.

[At this point in the hearing, Senator Chiles entered the hearing room.]

Mr. O'Brien. So the procedures, I feel, are quite effective at our corporate level in that kind of situation.

Senator Nunn. Let me move away from this specific case to a more general concern. Do you believe there is really any way we can adequately supervise and recheck on a periodic basis 4.2 million people in this country who are given access to classified material? Don't just sheer numbers themselves mitigate against any sensible and adequate program?

Mr. O'Brien. It certainly makes it a very, very difficult problem. I think the resources to reinvestigate those numbers of people at the secret level would be prohibitive.

Senator Nunn. Are you not very far behind in the reinvestigation even of top secret people?

Mr. O'Brien. Yes, sir.

Senator Nunn. How far behind are you on top secret reinvestigations, according to your own criteria?

Mr. O'Brien. Well, at the present rate, we figure it would take us probably around 10 years to do a periodic reinvestigation on everyone with top secret.

Senator Nunn. Does that mean in 10 years, you will be caught up, or is there a whole other backlog coming.

Mr. O'Brien. That would take into account those coming in during that time.

Senator Nunn. Ten years from now you would be caught up on reinvestigation of top secret?

Mr. O'Brien. At our present pace. As I mentioned in the statement, we now have the idea of a quota system on initial request. This would cut down initial requests.

Senator Nunn. Is that in the industrial sector also or in the Government service?

Mr. O'Brien. Across the board. And we would use that additional investigative resource that would be freed up to concentrate on the periodic reinvestigations. So our hope is to put more effort on the periodic reinvestigatons and speed up that process.

Senator Nunn. Back to the specifics. We understand that Ruby Schuler and James Harper began removing classified documents from a corporation known as Systems Control Inc.—I will refer to it as SCI from here on—for sale to Polish agents as early as May 1979. According to DIS files, DIS inspected SCI security twice before Harper was arrested and once immediately afterwards.

In November 1982, the DIS inspection found "overall security posture to be good." In May 1983, DIS again found security posture to be good. Harper was arrested in October 1983. In December 1983, after Harper's arrest, DIS found security to be poor. [Laughter.]

What happened in the interim and what went wrong in the early investigations, or what was revealed in the latter investigation?

Mr. O'Brien. For the latter investigation, we sent people from Washington. It was a very intensive investigation where we really turned the thing inside out. Before that, of course, we conducted our normal inspection. No facility or Government activity is better than the weakest link in its chain, and if there is an individual who elects to commit espionage, there is really very little that we can do. We set up a system of procedures and control——

Senator Nunn [interposing]. I understand that, but in December 1983, you found the system itself to be poor.

Mr. O'Brien. That's after we knew there had been a problem. As I say, we had a high-level team in from Washington and we really turned the place inside out.

Senator Nunn. What do you go into normally?

Mr. O'Brien. In that particular facility, we would go in with a team of probably two or three people. We did find some problems there. We found they were retaining classified material on contracts that had been completed, and they should have been destroying the material or returning it to the Government. We were pursuing that issue with them, and they were starting to reduce their inventories of classified.

Senator NUNN. As a consequence of that kind of investigation, moving from good to poor based on case history, and I understand how that can happen, but the system, if it was poor in December, it undoubtedly was poor the other three times you inspected it; wouldn't you conclude that?

Mr. O'BRIEN. Yes, sir; I would.

Senator NUNN. Just didn't find it?

Mr. O'BRIEN. I would agree with you.

Senator NUNN. Does that mean you don't have adequate inspections on a routine basis and, if so, have you done anything about it?

Mr. O'BRIEN. I don't accept the premise. I think our inspections are good. I've got about 280 industrial security representatives who spend a lot of time on training. They are trained for about a year before they are off on their own. We have a lot of continuing training effort. We emphasize the quality of our inspections, and I feel, generally speaking, our inspections are very good. You have to take into account, this year we are going to conduct 22,400 inspections, and some are very, very large facilities where we send a team of maybe 10 or more people in for as much as 3 weeks—are the procedures generally working; are the security systems working—and we can assess that pretty well. I think by and large we do a pretty good job.

Senator NUNN. This gets to the question about incentives. What incentives does a contractor have to take good security measures to really ensure security is good? What are the incentives in terms of the all-American measurement stick of bottom-line profit?

Mr. O'BRIEN. The bottom-line incentive, if we declare a facility unsatisfactory, that then makes the company ineligible for any additional classified work. So that goes right to the economic heart of the matter.

Senator NUNN. How many times have you done that in the last 12 months?

Mr. O'BRIEN. I don't have the number, but I would say in the neighborhood of 15 to 20.

Senator NUNN. Out of how many?

Mr. O'BRIEN. Out of 14,000.

Senator COHEN. Major facilities?

Mr. O'BRIEN. Some major facilities; yes, sir.

Senator NUNN. It would be very hard to take that step, wouldn't it, against very large contractors on a production basis or are you independent?

Mr. O'BRIEN. We are very independent. If we find a situation unsatisfactory, we take the action.

Senator NUNN. Who has to approve that? When you say "we," at what level? Is that your responsibility?

Mr. O'BRIEN. My regional director.

Senator NUNN. Regional director.

Mr. O'BRIEN. Right.

Senator NUNN. Who has to approve that?

Mr. O'BRIEN. My regional director.

Senator NUNN. Does that mean all work stops at that stage?

Mr. O'BRIEN. No, sir. Here is what it means. First of all, we announce to all contracting activities that the contractor's facility clearance is now unsatisfactory. We tell them they may not send additional classified material to that facility. Each procuring activity can decide with respect to ongoing contracts whether or not they want to continue.

Let's say a particular Navy contract is 95 percent finished. Well, all things considered, the Navy might let them finish this work but they can't get anything else.

Senator NUNN. They have to correct it, though, before they are eligible for additional contracts?

Mr. O'BRIEN. Yes; what we usually do is give them 30 days to get their house in order. We go back in with a followup inspection in 30 days, sometimes sooner, depending on the nature of the problem, and we really get them cracking.

Once that happens, we get a lot of attention and usually get the problems fixed quite quickly.

Senator COHEN. Can you give us a list of those facilities that have been denied their clearance in the last 12 months?

Mr. O'BRIEN. Yes, sir.

[The information referred to follows:]

DISP FACILITIES RATED UNSATISFACTORY - FY 84

COMPANY	DATE UNSATISFACTORY	DATE RESTORED TO SATISFACTORY
Amex Systems, Inc. 2311 El Segundo Blvd. Hawthorne, CA 90250	August 14, 1984	September 21, 1984
Analysis & Technology Inc. Rt. 2, Technology Park North Stonington, CT 06359	April 20, 1984	May 14, 1984
EDO Corporation Western Division 2645 South 300 West Salt Lake City, UT 84115	February 14, 1984	February 22, 1984
Global Analytics Inc. 10065 Old Grove Road San Diego, CA 92131	June 19, 1984	July 20, 1984
Houdaille Industries, Inc. Warren Pumps Division Bridges Avenue Warren, MA 01083	January 31, 1984	March 9, 1984
Hughes Aircraft Co. Missile Systems Group Tucson Mfg. Division Nogales Highway Tucson, AZ 85706	November 15, 1983	December 8, 1983
Infrared Industries, Inc. 12151 Research Parkway Orlando, FL 32856	June 19, 1984	Term December 14, 1984
Lehigh Design of NESCO Design Group Inc. 4130 North Marshall Way Scottsdale, AZ 85251	January 27, 1984	April 30, 1984
Pace Publications Arts, Inc. 3531 Miraloma Avenue Anaheim, CA 92803	July 12, 1984	Term January 24, 1985

Paragon Design Co., Inc. 3574 Kettner Blvd. San Diego, CA 92601	August 14, 1984	------
Raytheon Co. Boston Post Road Wayland, MA 01778	December 20, 1983	January 26, 1984
R-Way, Inc. 307 E. New Haven Avenue Melbourne, FL. 32901	March 27, 1984	Term September 4, 1984
Soladyne Inc. 7447 Convoy Court San Diego, CA 92111	January 25, 1984	April 27, 1984
Roger White Associates Inc. 993 Shockney Drive Ormond Beach, FL 32074	September 21, 1984	October 24, 1984

DISP FACILITIES RATED UNSATISFACTORY - FY 85

COMPANY	DATE UNSATISFACTORY	DATE RESTORED TO SATISFACTORY
General Dynamics Corp. Convair Division 5001 Kearny Villa Road San Diego, CA 92138	October 5, 1984	November 19, 1984
General Dynamics Corp. Pomona Division Rockaway Field Office 200 E Main Street Rockway, NJ 07866	March 25, 1985	-------
Rockwell International Corp. Missle Systems Division 1800 Satellite Blvd. Duluth, GA 30136	March 13, 1985	-------
Sonicraft, Inc. 8859 South Greenwood Ave. Chicago, IL. 60619	November 9, 1984	January 28, 1985
Sparton Electronics Florida, Inc. Johnson Lake Road DeLeon Springs, FL 32028	February 28, 1985	-------
Stanford Telecommunications, Inc. 2421 Mission College Blvd. Santa Clara, CA 95054	January 25, 1985	February 1, 1985
Tracor Applied Sciences, Inc. Inglewood Office 11222 S La Cienega Inglewood, CA 90304	March 12, 1985	-------

Senator NUNN. The DIS inspections that we were referring to in the SCI case found visit control satisfactory; the December report found "no deficiencies during the night and weekends inspection," yet the FBI tells us that Schuler, as well as Harper, who was uncleared at that time, had free access to areas holding classified documents after hours and on weekends.

We also understand that there is still today no after hours monitoring of access to classified areas at SCI, now known as SCT. Whether this is correct or not, I would like to ask you. The same problem, of course, has been well documented in the Boyce case, and we will be hearing about that from TRW. How about after-hours access, what is your standard there, and what has happened at SCT since then?

Mr. O'BRIEN. We require after hours, that classified material be properly secured in containers or closed areas where access can only be obtained by people that have a proper clearance and need to know.

Now again, we are talking about 14,000 cleared facilities; many are very small companies. They have to lock the material in a safe generally at night. And there are procedures if a cleared person needs to work on a weekend, on a Saturday, they can go in and open the safe and do the work they have to do.

So those procedures are there. If a cleared individual elects to be a traitor, we just can't have somebody watching 1.4 million people all the time.

Senator NUNN. I understand that, and I understand there is no such thing as a perfect system, as Senator Cohen said. The after-hours access is a problem that has been documented over and over again in these cases.

My question is, do you believe you have adequate procedures to cover that?

Mr. O'BRIEN. We are working to see if we can improve those further, but the problem is that if we tell a company, let's say we say there has to be at least two men present, one of the ways to do it is you have two people before you can open the safe during nonworking hours. That would have a big economic impact on a lot of people. A lot of engineers come in and work on a Saturday, particularly a lot of small companies like the one where Ms. Schuler was. If one person can't work, you have to have two, you are talking a lot of dollars.

Those are the sort of things which must be considered—what is the right balance?

Senator NUNN. We are going to be hearing from Christopher Boyce in a few minutes. Of course, he was granted secret clearance very quickly and later top secret clearances through the Government at TRW. I expect him to testify, and I think some of the published material on his case and Daulton Lee's case indicate that the security check was woefully inadequate, at least from his perspective.

None of his peers, none of the people he was with, none of his own age group were questioned at all; just primarily his parents, his minister, so forth.

Is that a normal procedure in a DIS check? If the Boyce case were coming up today, if you were being asked for a top secret clearance for someone like him, what would you do to check it?

Mr. O'BRIEN. Boyce was investigated by CIA, who also had the security inspection responsibility, not DIS.

Senator COHEN. Should we worry about that?

Mr. O'BRIEN. Pardon me?

Senator COHEN. Should we worry about that? [Laughter.]

Mr. O'BRIEN. I would not attempt to tell the committee what to worry about. [Laughter.]

One of the lessons learned in the Boyce case was the emphasis we need to put on peer coverage, and since then, we have been directing our investigative peer coverage as opposed to friends, parents, that kind of thing.

Senator NUNN. Do you think you would at least have talked to his peers if that came up again today?

Mr. O'BRIEN. Yes, sir; I am confident we would.

Senator NUNN. One other question, and I will defer to my colleague. We have to move along here, and I have many questions for the record. Allegations have been made about various disparities between DIS' service and OPM's service. Mr. Devine said the other day that the Office of Personnel Management, even though their costs are higher, No. 1, does not have the same luxury as DOD or DIS in not absorbing overhead. Does DIS get a free overhead ride in your charges to agencies?

Mr. O'BRIEN. No, sir; we do not. I have a finite amount of dollars, and most of our offices are in Federal buildings or in commercial buildings where we pay rent. We have some offices on base, and we have support agreements whereby we have to reimburse the hosts for the services that they provide us.

Senator NUNN. In other words, you are saying all the overhead is reflected in your billing to the various customers you have?

Mr. O'BRIEN. We don't bill. OPM operates on an industrial-funded basis, where we operate on a straight-budget basis. There is no exchange of funds. We just have a set amount of our budget——

Senator NUNN [interposing]. If we are trying to compare how much it costs for you to do your investigation with how much it costs to do OPM's investigation, how do we do that? Is there a meaningful comparison?

Mr. O'BRIEN. Yes. DIS conducts investigations at far less cost than OPM.

Senator NUNN. Why is that? They say it is because you don't have to pay overhead, and you don't charge retirement, so forth, so on; is that right?

Mr. O'BRIEN. No, sir; no, sir. We pay everything they pay. In fact, that's been looked at by the General Accounting Office. I think the same dollars they have to expend we have to expend.

Senator NUNN. Does this mean DIS is much more efficient than OPM?

Mr. O'BRIEN. I would have to assume that; yes, sir.

Senator COHEN. Doing a quicker job at less expense.

Mr. O'BRIEN. Yes.

Senator NUNN. That gets to the next point, exactly, Mr. Chairman. OPM says, well, if it is more expensive, it is because we do twice as many checks; DIS doesn't do as many checks as we do, we do a more thorough job; do you have any comments on that?

Mr. O'Brien. Yes, indeed, I do. Our investigations, very frankly, are better, and I say that without fear of equivocation. They have a different philosophy. Theirs is how many people do I talk to and our thought is how well do we talk to them.

For example, every one of our agents, and we are very selective in whom we hire have a very structured training program. Now they are in an office for at least 3 weeks OJT, and then we have a 4-week school in Richmond, VA. OPM sends theirs to 1-week training. We have 4 weeks and then we have a continuing, very active continuing education program. And we stress, as our central theme, the indepth interview of the subject, and we get a great deal out of that.

OPM, I understand, is just now going to or considering doing subject interviews. I've looked at this very, very hard and my honest opinion is that our investigation is the best background investigation—IBI—conducted in Government today.

Senator Nunn. Mr. Chairman, I will offer the rest of my questions for the records. We appreciate very much your cooperation.

Senator Cohen. OPM is to follow you. Senator Gore.

Senator Gore. Thank you, Mr. Chairman. I will try to keep my questions short. I did want to follow through on the interaction between you and OPM and discuss briefly with you the basic installment 311. Secretary Weinberger has indicated DOD is not very happy with basic installment 311 and would prefer all agencies cooperate with the NSDD-84 effort.

Does DOD believe that basic installment 311 affects directly or indirectly not just suitability but security as well?

Mr. O'Brien. Very honestly, Senator, from the Defense Investigative Service, I have not been involved—I'm an administrator, not a policy person. General Stilwell will be here later today——

Senator Gore [interposing]. I will ask General Stilwell about that.

Let me ask you another question then. You were talking with Senator Nunn about the option you have of cutting off all work to contractors, shutting them down if they violate the security procedures. Would you agree that it might make sense to have another option short of this extreme measure that officials are understandably and often reluctant to use? Something like a fine that would penalize them financially?

Mr. O'Brien. We do have another option. In fact, when we do an inspection, if we call them unsatisfactory, that is the worse end of the spectrum. If we find major deficiencies, we brief top management and point out major deficiencies. If they don't take corrective action quickly, then we will go to unsatisfactory; 3 percent of our inspections result in major deficiency findings and are corrected before it gets that bad.

Senator Gore. You have the option of shutting them down, and you have the option of telling them you may shut them down if they don't improve. But wouldn't something else be helpful, too, to tell them, look, you messed up here; we're going to fine you and it's going to cost you *x* number of thousands of dollars?

Mr. O'Brien. We really don't have a problem. As a matter of fact, we approach this industrial security program as a partnership with industry. The numbers of people we have in DIS are very, very small compared to the big mass contractors involved in classified work.

We try to work with them. We put a lot of emphasis on training. They are trying to do a good job 99.9 percent of the time and they are working with us. We really have not found the need—

Senator Gore [interposing]. I just can't agree with you when you say we really don't have a problem.

Mr. O'Brien. Most of these contractors are doing a very good job. There are always going to be espionage cases. I don't think we can put a hundred percent stop to that.

Senator Gore. You don't believe you need another tool?

Mr. O'Brien. I don't believe so. I will be glad to study it and look at it.

Senator Gore. I wish you would. If you want to add to your response for the record, I will be glad to hear it. I disagree with you, and I think the evidence indicates the problem is quite severe.

[The information referred to follows:]

We have reviewed this subject and still believe another tool, i.e. monetary fines or other penalties, would not appreciably aid us in our mission and may, in fact, serve to our detriment. The "ideal," of course, would be to have all contractors maintain a security-violation free environment and we constantly emphasize the need to prevent violations. However, we also emphasize the need to surface and report all violations as they occur so that we can review the circumstances and ascertain the impact on national security. This is based on the premise that the one thing worse than a compromise of classified information is a compromise which we don't know about. In view of the volume and complexity of industry's classified involvement, the Government will never have enough resources to "uncover" every violation on their own. We are highly dependent upon contractors to report violations on themselves and, for the most part, believe that we have created an environment where most contractors feel free to do so. Initiation of monetary fines or other punitive measures can only serve to discourage industry from reporting their own mistakes with the very undesirable result that significant compromises of classified information would be unreported.

Senator Gore. Also, the record indicates, that you simply can't do the job at the present time for getting your clearances back on time and doing the rechecks that are advisable.

Mr. O'Brien. We are completing our background investigations on an average of 90 days. I am expecting that to improve in the next several months.

Senator Gore. You can't do the rechecks?

Mr. O'Brien. The periodic reinvestigations are a problem.

Senator Gore. Why not give the contractors responsibility for updating rechecks?

Mr. O'Brien. To have 14,000 contractors doing investigations on their people is a concept we really haven't considered. We can certainly look into that. At this time, I feel the investigation is a province of the Government. I think, as a general rule, it should remain so.

Senator Gore. You are relying on them for an awful lot of other things.

Mr. O'Brien. I should point out one additional thing that hasn't been mentioned. We have a very active program, a requirement that every contractor report any adverse information coming to their attention involving their people, and we pursue that aggressively. So that whenever a contractor learns that a person has an alcoholic problem, drug problem, financial problem, they report that to us, and in these cases; we initiate an investigation immediately.

Senator **Gore**. There are so many examples where those reports just are not made. General Dynamics did not report that on the Veliotis case.

Mr. **O'Brien**. That's true. They are not made 100 percent. However, we really keep on them.

Senator **Gore**. Not close enough, I would say. We will puruse that issue with other witnesses, the option of assigning some of this responsibility for rechecks to contractors. I know the contractors are opposed to it, but there may be some strong arguments in favor of that.

Mr. Chairman, in the interest of time, I am going to cut off my questions. Thank you very much.

Senator **Cohen**. Senator Chiles.

Senator **Chiles**. I have no questions.

Senator **Cohen**. Mr. O'Brien, thank you very much. You have been very helpful to the subcommittee.

Mr. **O'Brien**. Thank you very much.

Senator **Nunn**. Thank you, Mr. O'Brien.

[Mr. O'Brien's prepared statement, with attachments, and responses to written questions follow:]

PREPARED STATEMENT OF THOMAS J. O'BRIEN

Mr. Chairman,

I am pleased to have this opportunity to discuss the mission of the Defense Investigative Service with this committee.

The Defense Investigative Service (DIS) is designated under its Charter, Department of Defense Directive 5105.42, as a Criminal Justice, Personnel Security Investigative and Industrial Security Agency. We report to the Under Secretary of Defense (Policy). We are responsible for conducting all personnel security investigations for the Department of Defense. These investigations are necessary to determine eligibility for security clearance, and they involve military, civilian, and industrial personnel. This year we will conduct approximately 220,000 such investigations and, in addition, we will complete 900,000 National Agency Checks. DIS also conducts investigations of unauthorized disclosures of classified information and other investigations as directed by the Under Secretary of Defense (Policy).

Our second major mission is the administration of industrial security. Three programs are involved. The largest is the Defense Industrial Security Program which provides the framework for ensuring that classified information entrusted to industry is properly safeguarded. This program involves not only the Department of Defense contractors, but also 18 other departments and agencies of government for which DIS provides industrial security administration. There are over 14,000 cleared contractor facilities employing approximately 1.4 million persons who have been cleared for access to classified information. The second program is the Industrial Facilities Protection Program. Under this program, key facilities essential for industrial mobilization are identified. DIS surveys these facilities to provide advice and counsel on their physical security posture and contingency planning.

Finally, DIS also provides security oversight for those Department of Defense contractors who have sensitive arms, ammunition, and explosives in their custody in connection with contract performance.

DIS resulted from a 1970 Blue Ribbon Committee Report, which stated that personnel security investigation work was a non-combatant function, in which some consolidation within DoD might lead to savings. Thus the DoD Personnel Security function which had previously been accomplished by the Army Intelligence Command, the Naval Investigative Service, and the Air Force Office of Special Investigations, became centralized in a single organization, the Defense Investigative Service, on October 1, 1972. The consolidation was responsible for saving 378 personnel spaces, 395 operating facilities, 244 vehicles and, of even greater importance, led to far greater uniformity of the investigative product.

Initially authorized 3,000 personnel, 1,750 of whom were military, and organized into 20 districts, DIS was an organization whose manpower, physical plants and operational structure were almost entirely borrowed from the Army, Navy and Air Force. Gradually over the ensuing twelve years DIS evolved into the complete security organization it is today. This consolidation has proven to be most effective. Although our workload increased by 40% between 1973 and 1984, the total human resources applied to the mission were reduced during this period by almost 15% (Chart I). In 1980 the Industrial Security Program was transferred to DIS from the Defense Logistics Agency. The military personnel were gradually returned to their parent services and today DIS is an entirely civilian organization, authorized 3,693 personnel, and has a budget for fiscal year 1985 of $117 million.

Today DIS consists of Headquarters in Washington, DC; the Personnel Investigations Center in Baltimore, Maryland; the Office of Industrial Security International, with offices in Brussels, Belgium, Mannheim, Germany and Yokohama, Japan; the Defense Industrial Security Clearance Office In Columbus, Ohio; the Defense Security Institute in Richmond, Virginia; and nine regions with regional headquarters in Boston, Philadelphia; Washington, Norfolk; Chicago, New Orleans; San Antonio, San Francisco and Los Angeles.

With regard to personnel resources, I think it interesting to mention the turbulence which existed within DIS for many years. While DIS was initially authorized 3,000 personnel to perform but a single function, personnel security investigations, that figure was gradually reduced until it reached a low of 1,740 in 1979. It was not until November 1980 that the first major increase in PSI space authorizations was received. A net gain of 668 Personnel Security Investigations spaces took place in fiscal year 1983; however, we received a reduction of 105 spaces in fiscal year 1984. Adding the transfer of the Industrial Security Program into the agency and some additional resources provided for that program, the authorized strength is now 3693. Broken down by program element, there are 185 in the Headquarters, 2646 in the Investigative Program and 862 in the Industrial Security Program.

Because of reduced resources and a significant increase in requests for investigations, especially those of contractor employees, a category which jumped from 13% in fiscal year 1975 to a current rate of 37% (Chart II), we found ourselves with a pending caseload of over 84,000 investigations and completion times for Special Background Investigations alone averaging 197 days in 1981. In May 1981, as a first step toward reducing that backlog, the Deputy Secretary of Defense placed a moratorium on Periodic Reinvestigations, and later that year we received the net gain of 668 PSI spaces I mentioned earlier. Both of these factors contributed significantly to reducing the backlog and completion times, and by the end of fiscal year 1983, the backlog was down to about 36,000 cases and completion times were averaging about 70 days. Both of these numbers started to increase again during fiscal year 1984 due to the start-up of the Periodic Reinvestigation Program and enhancement of the Interview Oriented Background Investigation during the last half of fiscal year 1983. Our pending caseload as of the end of the 2nd Quarter fiscal year 85 was about 56,000 and the completion times for the same period were averaging 92 days overall and 85 days for cases in which there are no overseas leads (Chart III). Because of this increased workload and the completion times associated with it, the President's budget for fiscal year 1985 provided a strength of some 320 above that authorized for fiscal year 1984, with a budget of $117 million. An additional 53 spaces are programed for fiscal year 1986, with a budget of $123 million. Some of these increased personnel resources are for the Industrial Security Program, which you will note later in my testimony is also experiencing an explosive growth in workload.

During fiscal year 1984, DIS completed about 195,000 investigations. This figure was up from 182,000 in fiscal year 1983; 181,000 in fiscal year 1982; 155,000 in fiscal year 1981 and 143,000 in fiscal year 1980. As impressive as this increase in productivity has been, it fell short by 12,000 of completing the 207,000 investigations that were requested during fiscal year 1984. For fiscal year 1985, we are projecting 219,000 requests for investigation, of which about 30,000 will be Periodic Reinvestigations. Based upon that level of requests, we anticipate our backlog will be about 63,000 and completion times will exceed 100 days by the end of the fiscal year, unless additional resources are provided or there is a curtailment in requests for new investigations. To give you an idea of how we stand in relation to other Federal Government organizations which also conduct personnel security investigations, the Office of Personnel Management, which is the next largest, conducts only about twenty percent of the investigations we do.

We have initiated several major new programs to enhance security. First, I would like to discuss the Interview Oriented Background Investigation (IBI). We received authority to begin using this innovative type of background investigation in 1981, and it represented the first time since World War II that a major change has been made in the conduct of Personnel Security Investigations. One of the factors necessitating this change has been the drying up of traditional sources of information, most significantly refusals by many states or local jurisdictions to allow our Agents to have access to Criminal Justice Records. Other major factors are increased social mobility and general public fears of liability under privacy legislation. The IBI was implemented to offset these problems. The primary difference from other investigations is that this investigation contains an interview of the subject of the investigation, which is conducted early in the investigation. After all, who is in a better position to know the subject? Further, this approach is consistent with the Privacy Act, which requires that the government collect information to the greatest extent practicable directly from the individual concerned. We have found that these interviews produce information which the traditional references, neighborhood and educational checks fail to uncover. Also, the adjudicators in the Army, the Air Force and the Defense Industrial Security Clearance Office compared the results of this new investigation with the traditional Special Background Investigation over a period of eighteen months, and the Interview Oriented Background Investigation consistently developed more significant information. As a result, the IBI has gained widespread recognition and acceptance throughout the Department of Defense. We believe strongly that the IBI is a major step forward to meet the challenges.

The second enhancement to security occurred in 1983, when we began a major new program whereby Periodic Reinvestigations are conducted on personnel with Top Secret clearances and Sensitive Compartmented Information Access. While Periodic Reinvestigations were conducted for people with Sensitive Compartmented Information Access, prior to the moratorium of May 1981, which I mentioned earlier, they amounted to little more than a National Agency Check, which I will describe a little later. The scope of the new Periodic Reinvestigation, which includes a subject interview, as in the Interview oriented Background Investigation, actually exceeds the periodic reinvestigation requirements set forth by the Director of Central Intelligence in DCID 1/14 (Attachment IV) and it now applies to people with Top Secret clearances as well as those with Sensitive Compartmented Information Access. It is by far the most extensive periodic reinvestigation being utilized by the Federal Government today. The program is designed to identify those cleared people who may no longer be reliable or trustworthy. It is underscored by the fact that, in almost all instances in which cleared people have been found guilty of espionage, it is subsequently determined that they were not involved with foreign intelligence at the time they were initially investigated and cleared. Rather, their involvement in espionage developed after the initial investigation and clearance and after they were established in a position of trust. Hence, this new and aggressive reinvestigation program should serve as a deterrent to those who might otherwise become traitors.

With an organization as large as the Department of Defense, there is always the danger that more background investigations than absolutely necessary are being requested. DoD regulations provide that the level of access to classified information serves as the basis for an investigation. We are constantly on the alert to identify and discourage unnecessary requests for investigations. Although we have no foolproof way of ascertaining the validity of all requests that we receive, we do have limited mechanisms. General Stilwell met with senior representatives of the Military Departments to impress on them the high workload we have and to encourage them to reduce their requests for investigations. Our Headquarters staff and our Directors of Investigations in the field meet with the requesters and discuss with them the liabilities of requesting investigations for which there is no legitimate need. On the industrial side, our Industrial Security Representatives, as part of the periodic inspections of cleared facilities, review that overall Personnel Security Clearance Program to try to detect whether too many employees are being cleared. Admittedly, neither approach is wholly effective.

We have considered the concept of industrial funding as a means of controlling the PSI workload. However, we have found that it would be very costly for us to administer. We would have to maintain a large accounting staff to monitor the program, while short-run fluctuations in the demand for investigations would likely force us into crash recruiting drives to meet increasing demands and decreases in workload would result in potential reduction-in-force action. We have found that a quota system may be a more viable solution to controlling the workload. Such a system would not require a large administrative staff. In fact, we are currently administering a quota system for all periodic reinvestigations with no increase in overhead, and since the DoD components are already accustomed to this system, it would be much easier to implement than establishing an industrial fund. It should also be noted that a quota system would not be affected by the normal program and budget cycle. The Office of the Secretary of Defense (OSD) has recently proposed that a quota system be adopted and we are working closely with OSD in this effort. We are quite optimistic that a system to control requests for investigations will be put into effect in the near future.

The Department of Defense generally categorizes its Personnel Security Investigations as follows:

National Agency Check - This is exactly what the title implies — a check of the indices of appropriate national agencies. It always includes checks of the FBI Main File and Criminal Identification Division File as well as the Defense Central Index of Investigations. Other federal agencies are checked as appropriate such as: the Office of Personnel Management (OPM), the Immigration and Naturalization Service (INS), the State Department, Central Intelligence Agency (CIA), Military Personnel Records Centers, the various components of the Treasury Department, the National Guard Bureau, the Drug

Enforcement Agency (DEA), plus the files of other agencies when necessary. When adverse or questionable information is developed as a result of this record check, the investigation is expanded, as necessary, to develop all pertinent details. The National Agency Check, as a general rule, is used as the basis for the issuance of Personnel Security Clearances at both the Confidential and Secret levels. Because of ADP applications in DIS and in the other national agencies, this type of investigation is by far the least expensive.

Standard Background Investigation - This investigation, which includes a National Agency Check, has coverage in the field of such things as employment, education, references, developed references, credit and local criminal justice records in the area where the individual has lived, worked, or attended school. It covers the last five years of the subject's life, or since his or her eighteenth birthday if shorter, and is the basis for the issuance of the Top Secret clearance to DoD civilian personnel.

Interview Oriented Background Investigation - This investigation includes a National Agency Check, Local Agency Checks, a Credit Check, three employment and three developed references, an interview of the subject and selected scoping as required. It serves as the basis for the issuance of Top Secret clearances for military and industrial contractor personnel.

Special Background Investigation - This investigation is similar to the standard background investigation, except that, it covers the most recent fifteen years instead of the most recent five years. The scope of the Special Background Investigation is prescribed by Director of Central Intelligence Directive 1/14. This investigation is prerequisite to the issuance of Sensitive Compartmented Information Access.

Periodic Reinvestigation - This investigation includes a National Agency Check, Local Agency Checks, a Credit Check, an interview of the subject, employment and employment references, developed character references and selected scoping as required. It covers the last five years, and applies to all personnel with TOP SECRET clearances and those with access to Sensitive Compartmented Information. As I mentioned earlier, the scope significantly exceeds the periodic reinvestigation requirements set forth in DCID 1/14.

These investigations are all indexed in the Defense Central Index of Investigations, a 22 million record automated index of all investigative files held by the investigative components of the Defense Department. DIS is charged in its charter as executive agent for this index. It was created in 1965 at the direction of the Secretary of Defense, at which time the investigative files of the Army, Navy, and Air Force were listed. When DIS was established in 1972, responsibility for operation of the index was transferred from the Army to DIS, and since that time all DIS investigative files have also been included. While DIS is responsible for the operation of the index, each investigative component remains responsible for its listings.

It is important, in discussing investigations conducted by the Defense Investigative Service, not to paint too rosy a picture. Obtaining criminal justice history information, financial and education records is a formidable task these days. Federal statutes, such as the Privacy Act of 1974, the Family Education Rights and Privacy Act of 1974, the Right to Financial Privacy Act of 1978, as well as similar state statutes limiting access to records, are making that task of our investigators far more difficult and complicated today than ever before. Even where there are no legal impediments, attitudes and misunderstanding of the laws have created a reluctance or hesitation in both the public and private sectors so that there is less cooperation with DIS investigators.

Historically, most state and criminal justice agencies have afforded DIS open access to arrest records whether or not the case ultimately resulted in conviction. However, in recent years some jurisdictions have curtailed access to criminal history information. In some jurisdictions, we are now getting access only where there has been a conviction, and in others we are getting no information whatsoever. Generally speaking, the most significant problem is public policy in some jurisdictions--sometimes expressed in a statute-which precludes access on the theory that the criminal record may preclude an individual from obtaining employment or jeopardize their continued employment. The second reason is cost. Because of the volume of DIS investigations, some jurisdictions indicate that they can no longer absorb the cost of conducting criminal record checks on our behalf.

An individual's criminal record is an essential element in assessing their overall reliability to access to classified information. In the case of DIS, our subjects are already employed and to have the investigation is not a pre-employment check, but rather it is to determine simply if an individual is suitable for access to our national secrets. The appointment of an individual to a sensitive nuclear weapons position on a submarine without knowing of his prior arrest records is as significant as general police work in reviewing those same files for suspects in a felony case. Therefore, we have taken the initiative to have the DIS mission defined in Department of Justice regulations as truly Law Enforcement related. Of more consequence would be legislation recognizing the need for the Department of Defense to have full access to all relevant Criminal History Information. I believe that such access is critical to the effective performance of the DIS law enforcement mission and therefore to the protection of our national security.

DIS is working with each of the jurisdictions where problems are being encountered. In some cases we have had success, and in other jurisdictions we continue to have to close investigations without having access to this vital information. I consider this to be one of our most critical problems, and I feel that a concerted effort at the national level is necessary in order to bring state and local jurisdictions into a position of support of our overall national security priorities.

Because DIS investigators by virtue of their wide dispersal throughout the United States work only a portion of each investigation, we initiated an adjudicative feedback program to give the investigators results of adverse actions taken as a result of their investigations. This was done to provide our investigators with a full appreciation of their efforts and the overall direction of the PSI program, since roughly 8% of field investigations conducted by DIS result in some adverse action, such as revocation or denial of clearance. This program has been enthusiastically received by our agent corps and provides an enhanced sense of professionalism and accomplishment to all of our employees.

Within the Defense Industrial Security Program, we have seen an explosion in the need for security clearances. This results primarily from the defense build-up to include the acquisition of sophisticated high-technology weapons, and to a lesser extent, to contracting out under OMB Circular A-76. It does not appear that it will drop to former levels in the near future. There are now over 14,000 cleared industrial contractor facilities, a figure which has increased by over 3,000 in just the last four years (Chart V). These cleared facilities employ about 1.4 million employees who require access to classified information. To give you a feeling for the order of magnitude this creates in the security clearance field, during fiscal year 1984, DISCO issued 257,393 clearances, a 23.6% jump over FY83. For fiscal year 1985, DISCO will grant 306,000 clearances, a figure which is an 18.9% increase over FY84.

The Industrial Security Program is a very complex program, which involves the safeguarding of classified information entrusted to industry through contracts they have been awarded. Its authoritative basis is Executive Order 10865. At this time, Mr. Chairman, I would like to introduce as for the record, a copy of Executive Order 10865 and 12356 (Attachments VI and VII).

As mentioned earlier, we have seen the number of cleared facilities in the program grow by over 3,000 in just the past four years, to a figure in excess of 14,000. The impact this has had on DIS has been dramatic. Inspections of cleared contractors are required every six months for those with Top Secret and Secret material, and every nine months for all others. The increase in the number of required inspections, over 20,000 in fiscal year 1984, coupled with the labor intensive and time consuming nature of them, ranging from two - three weeks with a team of perhaps as many as eight personnel for a large facility, to a matter of hours by one person for a very small facility, has been very taxing on DIS resources. This problem is further amplified by the number of contractor facilities with ADP systems, currently just under 1,800, an increase of over 77% since the beginning of fiscal year 1982. The number of ADP systems at those facilities is of even greater concern, currently almost 10,000 systems, for an increase of over 129% since the beginning of fiscal year 1982.

Adding to complexity of the program has been the dramatic increase in the amount of foreign investment in the segment of U.S. industry engaged in classified government contracts. This is evidenced by a 33% increase in the number of facilities subjected to a formal determination during fiscal year 1984. The program precludes the issuance of a facility clearance to a contractor which is determined to be under foreign ownership, control or influence. There is an exception to this rule, which is based upon bilateral agreements with the United Kingdom, Canada, the Federal Republic of Germany, the Netherlands, Norway and Denmark. Where a significant degree of foreign ownership exists, a voting trust agreement or proxy agreement is suggested as a means of insulating the U.S. firm from its foreign parent. Under special circumstances, when a User Agency and the OSD determine that it serves our national interest, a foreign firm may be insulated through a special security agreement. This agreement, however, allows the foreign parent to retain control over the U.S. firm's operations and management.

The processing of these cases is very time consuming and detailed in scope, and involves action at both the field and headquarters levels. In addition to the recurring security inspections conducted on a regular basis, special foreign ownership, control and influence reviews are conducted each year for firms operating under a voting trust or proxy agreement to ensure compliance with all established special controls, practices and procedures. Further, at the end of each year of operation under either type of agreement, trustees or proxy holders are required to submit to DIS an annual report of agreement implementation, jointly compiled by the trustees or proxy holders and the Chief Executive Officer of the U.S. Facility. Thus as you can see, the Industrial Security Program, like the Investigative Program has been overwhelmed by increases in work requirements, which have far outpaced our ability to complete them unless additional resources are provided.

The Defense Security Institute, a component of DIS, trains all Special Agents and Industrial Security Representatives. Comprehensive courses of instruction of four and five weeks respectively, are provided to new personnel in these fields. Additionally, refresher training is conducted by institute personnel for our Agents and Industrial Security Representatives in order to keep them current on techniques and procedures as well as the laws and regulations which affect the Investigative and Industrial Security Programs. The Institute is also responsible for industrial security and information security training for other U.S. government personnel, employees and representatives of U.S. Government contractors, and selected foreign governments. During fiscal year 1984, the Institute provided training for 4,147 U.S. personnel and 13 foreign government personnel. This training consisted of 30 resident and 32 field extension courses. Additionally, the Institute had a grand total of 3,034 correspondence course enrollments and completions during fiscal year 1984. The correspondence course students are from within government and industry, and participated in courses dealing with automatic data processing systems, the Defense Industrial Security Program and physical security. The Institute is currently developing a three week basic security course at the direction of OSD. The course will cover basic introductory instruction in all aspects of the security profession, with the purpose of providing a common base of general security knowledge within DoD. It is targeted at civilians in the 080 security career field in grades GS-7 and 9, and military in grades E5 and above. Seven courses per year with approximately 30 students per class are currently being planned.

I think it significant to point out that the Defense Investigative Service does not make security clearance determinations except for its own assigned personnel and through the Defense Industrial Security Clearance Office (DISCO) employees of cleared contractors. The DoD regulation which set forth the Personnel Security Program has required the various components of the department to centralize their adjudicative functions. This has been completely done by the Army, in their Central Personnel Security Clearance Facility, located at Fort Meade, Maryland. The Air Force Security Clearance Office, located in the Pentagon, makes all security clearance determinations for the Air Force except for those involving Access to Sensitive Compartmented Information. That function is performed by the Air Force Intelligence Service, also located in the Pentagon. The Navy has a centralized clearance function for its civilian personnel, and its Sensitive Compartmented Information Access determinations are made by the Naval Intelligence Command and the Naval Security Group, all are located in the Washington area. For military personnel, the Navy is decentralized, with clearance determinations being made at command level, worldwide. As I have already mentioned, DISCO determines eligibility for security clearances of all contractor personnel. However, should DISCO be unable to make the clearance determination, the case is referred for adjudicative review by the Defense Legal Services Agency.

Our adjudicators at DISCO are subject to continuous on the job training from the date of their selection. During their fledging period, this training is concentrated and constant, on a one-on-one basis with an experienced adjudicator. Once the individual meets an acceptable skills level, the training reverts to group sessions where policies, procedures, and outcome are studied with case studies providing the educational vehicle. Formal training is also provided by sending selected adjudicators to courses conducted by other federal agencies.

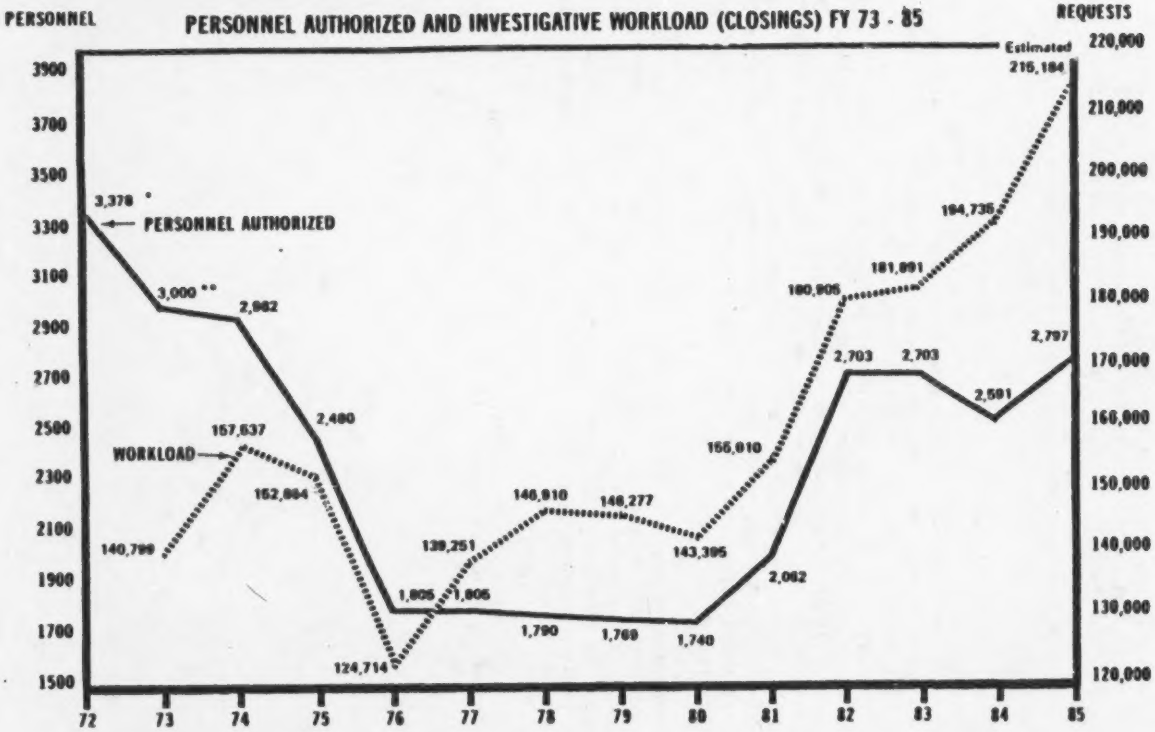
We feel it is unfortunate that so much emphasis has been placed on the role of investigations in the security clearance process, when in fact it is only a part, and probably not the most important part, of the personnel security process. The DoD relies a great deal on the requirement that there be a continuous evaluation of eligibility for clearance above and beyond the initial investigative requirement. There is a continuing security responsibility on the part of the supervisor, whether, military, civilian, or industrial contractor, to ensure that personnel security problems are recognized early so that timely action can be taken to avert the compromise of classified information. With only about 1,535 investigators in DIS, compared to about three million cleared personnel in DoD and industry, it is only through a total team effort, investigator, adjudicator and supervisor, that we can have a successful Personnel Security Program.

Personnel security is, in a way, like life insurance -- how much do we need, and how much can we afford? However, unlike a life insurance policy, wherein clear-cut events will eventually occur which prove the worth of the policy, it not so simple in the personnel security arena to know how well one's program is working -- that is to say, whether or not we have taken out sufficient insurance.

This completes my formal remarks. If you any questions, I will be happy to respond to them now. Thank you.

Percent Change in Workload FY 73 - 85 +52.8%
Percent Change in Personnel FY 73 - 85 – 6.8%

PERSONNEL AUTHORIZED AND INVESTIGATIVE WORKLOAD (CLOSINGS) FY 73 - 85

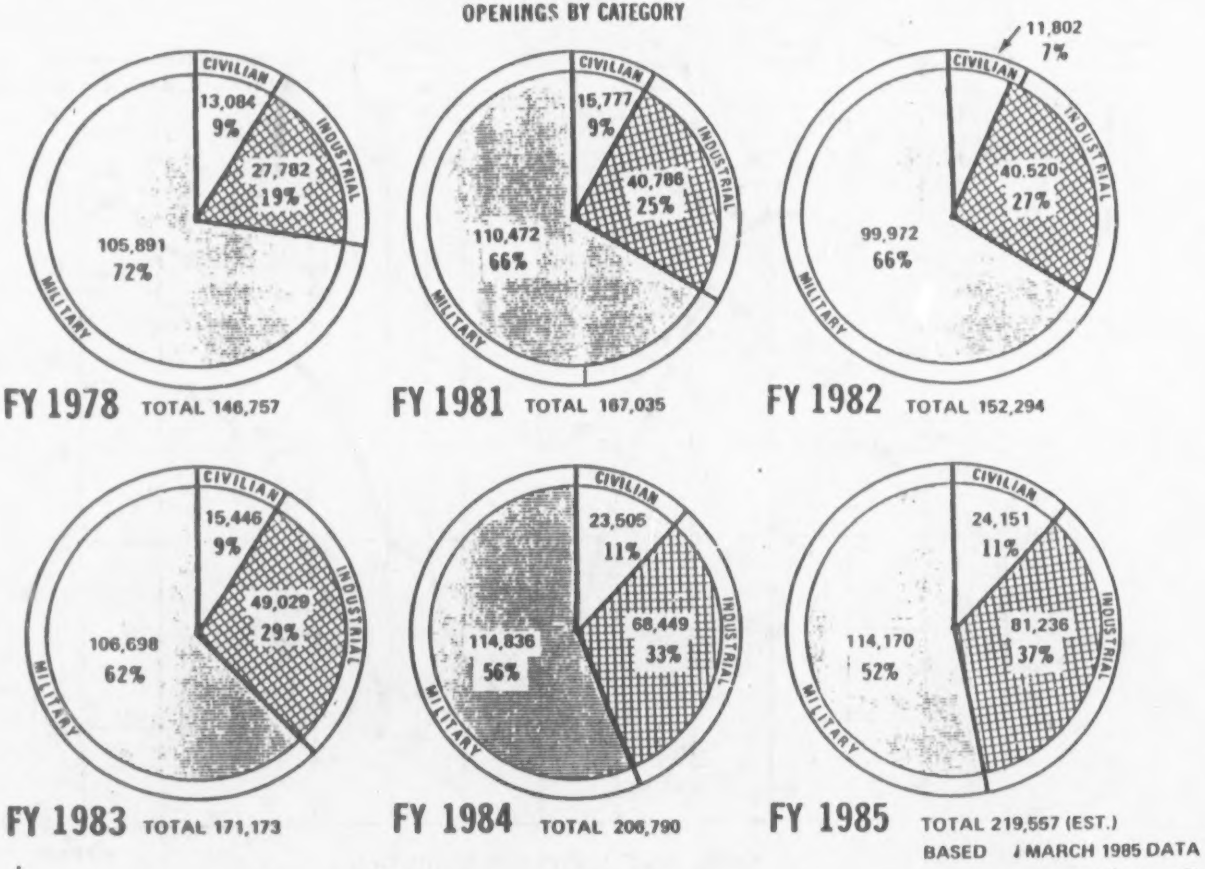


*Number of personnel identified by the Services for transfer to DIS.

** Number authorized to DIS

PERSONNEL SECURITY INVESTIGATIONS

OPENINGS BY CATEGORY



PSI PENDING AND COMPLETION TIMES

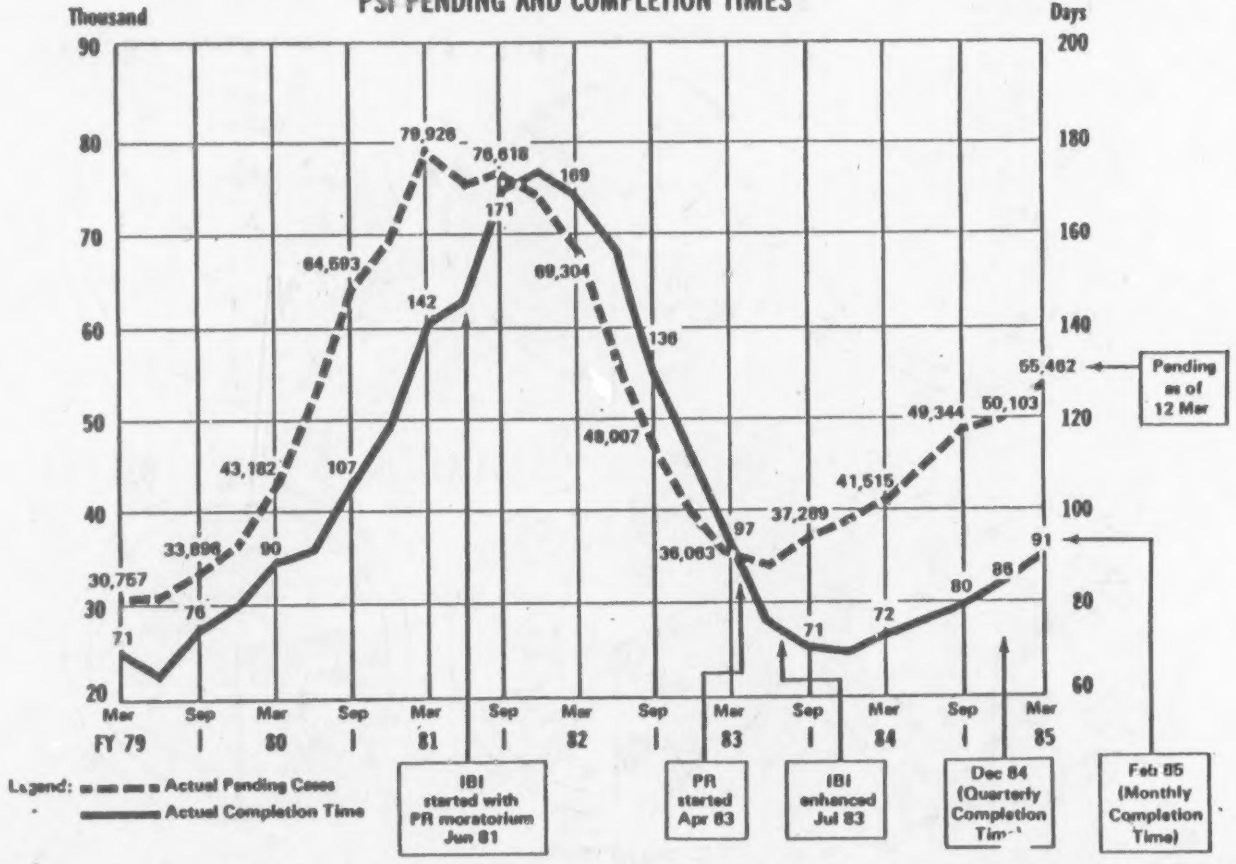


Chart III

Director of
Central
Intelligence

Director of Central Intelligence Directive No. 1/14

by the
Security Committee

SECOM-D-147
September 1981

DCID No. 1/14
13 May 1976

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/14 [1]

MINIMUM PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION

(Effective 13 May 1976)

Pursuant to the provisions of Executive Order 11905, Section 102 of the National Security Act of 1947 and National Security Council Directives, the following minimum personnel security standards, procedures and continuing security programs are hereby established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors and other individuals who require access to Sensitive Compartmented Information [2] (hereinafter referred to as SCI). The standards, procedures and programs established herein are minimum and the departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to ensure that effective security is maintained.

Purpose

1. The purpose of this Directive is to enhance the security protection of SCI through the application of minimum security standards, procedures and continuing security programs, and to facilitate the security certification process among Government departments and agencies.

Applicability

2. The provisions of the Directive shall apply to all persons (other than elected officials of the United States Government, federal judges and those individuals for whom the DCI makes a specific exception) without regard to civilian or military status, form of employment, official rank or position or length of service.

3. Individuals who do not meet the minimum security criteria contained herein and who are, therefore, denied access to SCI shall not, solely, for this reason, be considered ineligible for access to other classified information. Individuals whose access to SCI has been authorized as an exception granted in accordance with paragraph 7 below, shall not, solely for that reason, be considered eligible for access to other classified information.

---

[1] This directive supersedes DCID 1/14 approved 1 July 1968.

[2] The term "Sensitive Compartmented Information" as used in this Directive is intended to include all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include Restricted Data as defined in Section II, Public Laws 585, Atomic Energy Act of 1954, as amended.

General

4. The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in the several existing authorities which govern access thereto, and in accordance with the personnel security standards and procedures set forth in this Directive. All persons accountable under the authority of this Directive and given access to information (SCI) containing sources or methods of intelligence shall, as a condition of obtaining access, sign an agreement that they will not disclose that information to persons not authorized to receive it.

Personnel Security Standards

5. Criteria for security approval of an individual on a need-to-know basis for access to SCI are as follows:

a. The individual shall be stable, of excellent character and discretion and of unquestioned loyalty to the United States.

b. Except where there is a compelling need, and a determination has been made by competent authority as described in paragraph 7 below that every reasonable assurance has been obtained that under the circumstances the security risk is negligible:

(1) Both the individual and the members of his or her immediate family shall be US citizens. For these purposes "immediate family" is defined as including the individual's spouse, parents, brothers, sisters and children.

(2) The members of the individual's immediate family and persons to whom he is bound by affection or obligation should neither be subject to physical, mental or other forms of duress by a foreign power, nor advocate the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

6. In exceptional cases, the Senior Intelligence Officer (SIO) of the Intelligence Community organization, or his designee, may determine that it is necessary or advisable in the National interest to authorize access to SCI prior to completion of the fully prescribed investigation. In this situation such investigative checks as are immediately possible shall be made at once, and should include a personal interview by trained security or counterintelligence personnel. Access in such cases shall be strictly controlled, and the fully prescribed investigation and final evaluation shall be completed at the earliest practicable moment.

Exceptions

7. The exceptions to paragraph 5.b.(1)(2) above may be granted only by the SIO or his designee, unless such authority has been specifically delegated to the head of an office or organization as set forth in inter-departmental agreements. All exceptions granted will be common sense determinations based on all available information, and shall be recorded by the agency making the exception. In those cases in which the individual has lived outside of the United States for a substantial period of his life, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the

minimum investigative requirements, and judicious review of the information therein must be made before an exception is considered.

Investigative Requirements

8. The investigation conducted on an individual under consideration for access to SCI will be thorough and shall be designed to develop information as to whether the individual clearly meets the above Personnel Security Standards.

9. The investigation shall be accomplished through record checks and personal interviews of various sources by trained investigative personnel in order to establish affirmatively to the adjudicating agency complete continuity of identity to include birth, residences, education, employments and military service. Where the circumstances of a case indicate, the investigation shall exceed the basic requirements set out below to ensure that those responsible for adjudicating access eligibility have in their possession all the relevant facts available.

10. The individual shall furnish a signed personal history statement, fingerprints of a quality acceptable to the Federal Bureau of Investigation and a signed release, as necessary, authorizing custodians of police, credit, education and medical records, to provide record information to the investigative agency. Photographs of the individual shall also be obtained where additional corroboration of identity is required.

11. Minimum standards for the investigation are as follows.

a. Verification of date and place of birth and citizenship.

b. Check of the subversive and criminal files of the Federal Bureau of Investigation, including submission of fingerprint charts, and such other National agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records shall be conducted on those members of the individual's immediate family who are United States citizens other than by birth or who are resident aliens.

c. A check of appropriate police records covering all areas where the individual has resided in the US throughout the most recent fifteen (15) years or since age eighteen, whichever is the shorter period.

d. Verification of the individual's financial status and credit habits through checks of appropriate credit institutions and interviews with knowledgeable sources covering the most recent five (5) years.

e. Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5) year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

f. Confirmation of all employment during the past fifteen (15) years or since age eighteen, whichever is the shorter period but in any event the most recent two years. Personal interviews with supervisors and co-workers at places of employment covering the past ten (10) years shall be accomplished.

g. Verification of attendance at institutes of higher learning in all instances and at the last secondary school attended within the past fifteen (15) years. Attendance at secondary schools may be verified through qualified collateral sources. If attendance at educational institutions occurred within the most recent five (5) years, personal interviews with faculty members or other persons who were acquainted with the individual during his attendance shall be accomplished.

h. Review of appropriate military records.

i. Interviews with a sufficient number of knowledgeable acquaintances (a minimum of three developed during the course of the investigation) as necessary to provide a continuity to the extent practicable, of the individual's activities and behavioral patterns over the past fifteen years with particular emphasis on the most recent five years.

j. When employment, education or residence, has occurred overseas (except for periods of less than five (5) years for personnel on US Government assignment and less than ninety days for other purposes) during the past fifteen years or since age eighteen, a check of the records will be made at the Department of State and other appropriate agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas in order to cover significant employment, education or residence and to attempt to determine if any lasting foreign contacts or connections were established during this period. However, in all cases where an individual has worked or lived outside of the US continuously for over five years, the investigation will be expanded to cover fully this period in his life through the use of such investigative assets and checks of record sources as may be available to the US Government in the foreign country(ies) in which the individual resided.

k. In those instances in which the individual has immediate family members or other persons with whom he is bonded by affection or obligation in any of the situations described in subparagraph 5.b.(2), above, the investigation will include an interview of the individual by trained security, investigative or counterintelligence personnel to ascertain the facts as they may relate to the individual's access eligibility.

l. In all cases the individual's spouse shall at a minimum be checked through the subversive files of the Federal Bureau of Investigation and other National agencies as appropriate. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family to the extent necessary to permit a determination by the adjudicating agency that the provisions of paragraph 5, Personnel Security Standards, above, are met.

m. A personal interview of the individual will be conducted by trained security, investigative or counterintelligence personnel when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation.

12. Where a previous investigation has been conducted within the past five years which substantially meets the above minimum standards, it may serve as a basis for

granting access approval provided a review of the personnel and security files does not reveal substantive changes in the individual's security eligibility. If a previous investigation does not substantially meet the minimum standards or if it is more than five years old, a current investigation shall be required but may be limited to that necessary to bring the individual's file up-to-date in accordance with the investigative requirements set forth in paragraph 11 above. Should new information be developed during the current investigation which bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

13. Programs shall be instituted requiring the periodic reinvestigation of personnel provided access to SCI. These reinvestigations will be conducted on a five year recurrent basis, but on a more frequent basis where the individual has shown some questionable behavioral pattern, his activities are otherwise suspect, or when deemed necessary by the SIO concerned.[3]

14. The scope of reinvestigations shall be determined by the SIO concerned based on such considerations as the potential damage that might result from the individual's defection or willful compromise of SCI and the availability and probable effectiveness of other means to continually evaluate factors related to the individual's suitability for continued access. In all cases, the reinvestigation shall include, as a minimum, appropriate National agency checks, local agency (including overseas checks where appropriate), credit checks and a personal discussion with the individual by trained investigative, security or counterintelligence personnel when necessary to resolve significant adverse information or inconsistencies.

15. The evaluation of the information developed by investigation on an individual's loyalty and suitability shall be accomplished under the cognizance of the SIO concerned by analysts of broad knowledge, good judgment and wide experience in personnel security and/or counterintelligence. When all other information developed on an individual is favorable, a minor investigative requirement which has not been met should not preclude favorable adjudication. In all evaluations the protection of the national interest is paramount. Any doubt concerning personnel having access to SCI shall be resolved in favor of the national security. The ultimate determination of whether the granting of access is clearly consistent with the interest of national security shall be an overall common sense determination based on all available information.

Continuing Security Programs

16. In order to facilitate the attainment of the highest standard of personnel security and to augment both the access approval criteria and the investigate requirements established by this Directive, member departments and agencies shall institute continuing security programs for all individuals having access to SCI. In addition to security indoctrinations, these programs shall be tailored to create mutually supporting procedures under which no issue will escape notice or be left unresolved which brings into question an individual's loyalty and integrity or suggests the possibility of his being subject to undue influence or duress through foreign

---

[3] In DoD, an SIO may request, with the approval of the Secretary of Defense or his designee, more frequent reinvestigations under special circumstances.

relationships or exploitable personal conduct. When an individual is assigned to perform sensitive compartmented work requiring access to SCI, the SIO for the department, agency or Government program to which the individual is assigned shall assume security supervision of that individual throughout the period of his assignment.

17. The continuing security programs shall include the followings:

a. Security education programs to ensure that individuals who are granted access to SCI are initially indoctrinated and periodically thereafter instructed as to its unique sensitivity and that they understand their personal responsibility for maintaining eligibility for continued access to SCI rests with the individual. Therefore, the individual is encouraged to seek appropriate guidance and assistance on any personal problem or situation which may have a possible bearing on his eligibility for continued access to SCI, and security counseling should be made available. These instructions should be conducted by individuals having extensive background and experience regarding the nature and special vulnerabilities of the particular type of compartmented information involved.

b. Security supervisory programs to ensure that supervisory personnel recognize and discharge their special responsibility in matters pertaining to the security of SCI, including the eligibility for SCI access. Such programs shall provide practical guidance as to indicators which may signal matters of security concern. Specific instructions concerning reporting procedures shall be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned to neutralize his vulnerability.

c. Security Review Programs to ensure that appropriate security authorities invariably receive and exchange, in a timely manner, all information bearing on the security posture of persons having access to sensitive information. Personnel history information shall be kept current. Security and related files shall be kept under continuing review.

18. Whenever adverse or derogatory information is discovered or inconsistencies arise which could impact upon an individual's security status, appropriate investigations shall be conducted on a timely basis. The investigation shall be of sufficient scope necessary to resolve the specific adverse or derogatory information, or inconsistency, in question so that a determination can be made as to whether the individual's continued utilization in activities requiring SCI is clearly consistent with the interests of the national security.

Effective Date

19. This Directive supersedes DCID 1/14, 1 July 1968. Existing directives,[4] regulations, agreements and such other references governing access to SCI as defined herein shall be revised accordingly.

---

[4] These include pertinent provisions of the Clearance Standards and Investigation and Evaluation section of the Communications Intelligence Security Regulations.

GEORGE BUSH
Director of Central Intelligence

19 March 1980

ANNEX A

DCID 1/14 ADJUDICATION GUIDELINES

PURPOSE

This annex is designed to ensure that a common approach is followed by Intelligence Community Departments and Agencies in applying the standards of DCID 1/14. These guidelines apply to the adjudication of cases involving persons being considered for first time access to Sensitive Compartmented Information (SCI) as well as those cases of persons being readjudicated for continued SCI access.

ADJUDICATIVE PROCESS

The adjudicative process entails the examination of a sufficient period of a person's life to make a determination that the person is not now or is not likely to later become an unacceptable security risk. SCI access adjudication is the careful weighing of a number of variables known as the "whole person" concept. The recency of occurrence of any adverse incident, together with circumstances pertaining thereto, is central to a fair and uniform evaluation. Key factors to be considered in adjudication are the maturity and responsibility of the person at the time certain acts or violations were committed as well as any repetition or continuation of such conduct. Each case must be judged on its own merits and final determination remains the responsibility of the individual SIO. Any doubt concerning personnel having access to SCI shall be resolved in favor of the national security.

The ultimate determination of whether the granting of SCI access is clearly consistent with the interests of national security shall be an overall common sense determination based on all ~~available information~~. In arriving at a decision consistent with the foregoing, the adjudicator must give careful scrutiny to the following matters:

a. Loyalty
b. Close relatives and associates
c. Homosexual conduct and sexual perversion
d. Cohabitation
e. Undesirable character traits
f. Financial irresponsibility
g. Alcohol abuse
h. Illegal drugs and drug abuse
i. Emotional and mental disorders
j. Record of law violations
k. Security violations

Adjudicative actions concerning the foregoing items are examined in greater detail below.

LOYALTY

DCID 1/14 establishes the categorical requirement that, to be eligible for SCI access, an individual must be of unquestioned loyalty to the United States.

CLOSE RELATIVES AND ASSOCIATES

DCID 1/14 requires close examination by the SCI adjudicator when members of an individual's immediate family and persons to whom he/she is bound by affection or obligation are not citizens of the United States, or their loyalty or affection is to a foreign power, or they are subject to any form of duress by a foreign power, or they advocate the violent overthrow or unconstitutional alteration of the Government of the United States.

The adjudicator must assess carefully the degree of actual and potential influence that such persons may exercise on the individual based on an examination of the frequency and nature of personal contact and correspondence with and the political sophistication and general maturity of the individual.

A recommendation for access disapproval is appropriate if there is an indication that such relatives or associates are connected with any foreign intelligence service.

When there is a "compelling need" for SCI access for an individual whose family member is a non-U.S. citizen and the background investigation indicates that the security risk is negligible, an exception to paragraph 5b(1), (2) of DCID 1/14 may be recommended.

In some circumstances, marriage of an individual holding SCI access approval could present an unacceptable security risk. An individual is required to file an intent to marry and it is the responsibility of the SIO to advise the individual of the possible security consequences. If the individual marries a non-U.S. citizen, SCI access will be suspended until the case is readjudicated unless an appropriate investigation of the spouse, as required by Paragraph 11L of DCID 1/14, was conducted with favorable results. In readjudicating such cases, the same judgments and criteria as reflected in this section apply.

HOMOSEXUAL CONDUCT AND SEXUAL PERVERSION

DCID 1/14 requires that, to be eligible for SCI access, individuals must be stable, of excellent character and discretion, and not subject to undue influence or duress through exploitable personal conduct.

Sexual conduct can be a relevant consideration in circumstances in which the conduct indicates a personality disorder or could result in exposing the individual to direct or indirect pressure because of susceptibility to blackmail or coercion as a result of the deviant sexual behavior. Such behavior includes: bestiality, fetishism, exhibitionism, necrophilia, nymphomania or satyriasis, masochism, sadism, pedophilia, transvestism, and voyeurism, Homosexual conduct is also to be considered as a factor in determining an individual's stability and susceptibility to undue influence or duress.

In examining cases involving acts of homosexual conduct or sexual perversion, it is relevant to consider the age of the person, the voluntariness, and the frequency of such activities, the public nature and the recency of the conduct, as well as any other circumstances which may serve to aggravate the nature or character of the conduct. A recommendation for disapproval is appropriate when, in view of all available evidence concerning the individual's history of sexual behavior, it appears that access to SCI could pose a risk to the national security.

COHABITATION

Extra-marital cohabitation with a member of the opposite sex, in and of itself, does not preclude SCI access approval.

The identity of a cohabitant must be ascertained and a determination made if such association constitutes an unacceptable security risk based on the same criteria as in the section dealing with Close Relatives and Associates. Cohabitation with an alien, for example, requires the same scrutiny as marriage to an alien. Extra-marital sexual relations are also of legitimate concern to the SCI adjudicator when the potential for undue influence or duress exists.

UNDESIRABLE CHARACTER TRAITS

It is emphasized that an individual's lifestyle is examined only in an effort to determine whether a pattern of behavior exists which indicates that granting SCI access could pose a risk to national security. In cases where allegations have been reported which reflect unfavorably on the reputation of an individual, it is incumbent upon the SCI adjudicator to distinguish fact from opinion and to determine which negative characteristics are real and pertinent to an evaluation of the individual's character and which are unsubstantiated or irrelevant. Relevant negative characteristics are those which, in the adjudicator's informed opinion, indicate that an individual is not willing, able, or likely to protect SCI information. The adjudicator's personal likes or dislikes must not be permitted to affect the determination.

Examples of specific concern in determining whether an individual has undesirable character traits are any substantive credible derogatory comments by associates, neighbors and other acquaintances; any litigation instituted against the individual by such persons as a result of the individual's actions; or allegations of violations of law. A recommendation for disapproval would be appropriate for an individual who cannot be relied upon to obey rules and regulations.

In examining the circumstances of cases involving incidents of untruthfulness, the ajudicator must weigh all factors with particular emphasis on establishing the intent of the individual. Where an individual has tried to obscure pertinent or significant facts by falsifying data, i.e. on the Personal History Statement by either omission or false entry, such action should be weighed heavily against recommending access. Failure to disclose derogatory personal information, such as a court martial or serious crime, would appear to be intentional and, consequently, would warrant a recommendation for disapproval.

FINANCIAL IRRESPONSIBILITY

Financial irresponsibility represents a serious concern to the SCI adjudicator. Persons who have engaged in espionage for monetary gain demonstrate the hazard of granting SCI access to an individual with overly expensive tastes and habits or living under the pressure of serious debt.

A recommendation for disapproval is appropriate when there is a pattern of financial irresponsibility and it appears that an individual has not made a conscientious effort to satisfy creditors. In such cases, the adjudicator should determine whether the individual had been notified about the debts and whether they were legally valid or ultimately satisfied.

When the financial irresponsibility alone is not of such magnitude to warrrant disapproval, it may contribute to recommendation for denial of SCI access when there is other evidence of irresponsibility.

ALCOHOL ABUSE

The SCI adjudicator should examine any information developed relative to an individual's use of alcoholic beverages to determine the extent to which such use would adversely affect the ability of the individual to excerise the care, judgement, and discretion necessary to protect SCI information, The adjudicator should determine whether a pattern of impropriety exists, although one incident caused by alcohol abuse may be of such magnitude to warant a recommendation for disapproval.

In determining the security impact of a person's pattern of alcohol use, the adjudicator should consider the circumstances, amount and rate of consumption, the time and place of consumption, and the physiological and behavioral effect such drinking has on the individual. For example, does the individual's drinking result in absences from work or careless work habits? Does the individual become talkative, abusive or manifest other undesirable characteristics? Does the individual drink until intoxicated? Has the individual been arrested for any acts resulting from the influence of alcohol?

In the absence of conclusive evidence, additional insight may be available from appropriate medical authorities. If the individual acknowledges having an alcohol abuse problem and is seeking help, it may be appropriate to defer access determination and monitor the individual's progess for a year or so.

If, after considering the nature and sources of the information, the adjudicator determines that an individual's drinking is not serious enough to warrant a recommendation for disapproval of SCI access, it may be appropriate to recommend approval with a warning at the time of indoctrination that future incidents of alcohol abuse may result in SCI denial. The adjudicator may also recommend a reinvestigation of the individual's use of alcohol after an appropriate period of time has passed.

ILLEGAL DRUGS AND DRUG ABUSE

The SCI adjudicator should examine all allegation of an individual's use, transport, transfer, sale, cultivation, processing and manufacturing of hallucinogens, narcotics, drugs and other materials and chemical compounds identified and listed in the Controlled Substance Act of 1970, as amended. Consequently an individual's involvement in any of these activities is of direct concern to the SCI adjudicator in order to determine the individual's capability to exercise the care, discretion, and judgement required to protect SCI information. The use of these substances may lead to varying degrees of physical or psychological dependence as well as having a deleterious effect on an individual's mental state and ability to function.

Persons involved in drug trafficking, i.e., the commercial cultivation, processing, manufacturing, purchase or sale of such substances should normally be recommended for disapproval.

In cases involving the use of drugs, the adjudicator must consider the nature of the substance used and whether the use is experimental or habitual. The frequency, recency and circumstances surrounding said use are key elements. For example, has the individual used "hard" drugs or hallucinogens such as heroin, cocaine or LSD? Has the individual used drugs regularly or only on occasion? Does the individual currently use drugs? Does the individual regularly purchase drugs or participate merely when offered drugs by others? Has the individual's behavior been affected by the use of drugs and, if so, to what extent?

Once the judgment is made that an individual is a habitual user of any controlled substance (multiple use beyond the point of mere experimentation), a recommendation for disapproval is appropriate. Moreover, even experimental use of hard drugs or hallucinogens, such as LSD, could warrant a recommendation for disapproval.

EMOTIONAL AND MENTAL DISORDERS

DCID 1/14 requires that persons considered for access to SCI be stable and of excellent character and discretion. Emotional and mental disorders which interfere with an individual's perception of reality or reliability are of serious concern to the SCI adjudicator in determining whether an individual is able or willing to protect SCI information.

It is essential to obtain as much information as possible when an allegation has been made in this area. If feasible, the individual should be interviewed to obtain additional details. When appropriate, government psychological and psychiatric personnel should be consulted so that psychiatric or psychological data may be properly evaluated.

If a current emotional instability appears to be a temporary condition, for example, caused by a death, illness or marital breakup, it may be advisable to recommend postponing final action and rechecking the situation at a later date. This precludes a security disapproval for what may be a temporary condition which, when cured, would have no security implications.

Military and civilian personnel who decline to take medical/psychiatric tests when so directed by competent authority should not be recommended for SCI access.

RECORD OF LAW VIOLATIONS

In determining whether an individual is stable, of excellent character and discretion as required by DCID 1/14 for access to SCI, the adjudicator must weigh carefully any record of law violations by the individual. Although a pattern of repeated minor traffic violations could be significant, the adjudicator is principally concerned with more serious criminal violations or court actions reflecting adversely upon the individual's reliability or trustworthiness.

Each case involving convictions for criminal offenses must be considered from the standpoint of the nature and seriousness of the offense, the circumstances under which it occurred, how long ago it occurred, whether it was an isolated offense or a repeated violation of the law, the offender's age at the time, social conditions which may have a brearing on the individual actions, and any evidence of rehabilitation.

Any conviction for a felony will normally support a recommendation for disapproval. If the offense was committed many years prior, the individual has shown evidence of rehabilitation, and the investigation shows no other derogatory information, an approval may be considered. A large number of minor offenses, however, could indicate irresponsibility and may support an adverse recommendation.

SECURITY VIOLATIONS

Most security violations are caused by carelessness or ignorance with no intention of compromising security. However, the record of an individual responsible for multiple violations should be scrutinized. The individual's current attitude toward security should be confirmed with his/her supervisor. A pattern of violations may be sufficient ground for a recommendation for disapproval.

28 September 1981

ANNEX B

DCID 1/14 APPEALS

POLICY

1. This annex establishes common appeals procedures for the denial or revocation of access to Sensitive Compartmented Information (SCI) by entities of the Intelligence Community after adjudication pursuant to the provisions of DCID 1/14. This annex is promulgated pursuant to Executive Order 12036, Executive Order 12065, Section 102 of the National Security Act of 1947, and National Security Council Intelligence Directive No. 1. For the purpose of this annex, all references to DCID 1/14 include the basic document and all of its annexes. Any person who has been considered for initial or continued access to SCI pursuant to the provisions of DCID 1/14 shall, to the extent provided below, be afforded an opportunity to appeal the denial or revocation of such access. This annex supercedes any and all other practices and procedures for the appeal of the denial or revocation of SCI access. This annex shall not be construed to require the disclosure of classified information or information concerning intelligence sources and methods, nor shall it be construed to afford an opportunity to appeal prior to the actual denial or revocation of SCI access. In addition, the provisions of DCID 1/14, this annex, or any other document or provision of law shall not be construed to create a property interest of any kind in the access of any person to SCI. Further, since the denial or revocation of access to SCI cannot by the terms of DCID 1/14 render a person ineligible for access to other classified information soley for that reason, the denial or revocation of SCI access pursuant to the provisions of DCID 1/14 and this annex shall not be construed tocreate a liberty interest of any kind.

APPLICABILITY

2. This annex applies to all United States Government civilian and military personnel, as well as any other individuals, including contractors and employees of contractors, who are considered for initial or continued access to SCI. This annex does not apply to decisions regarding employment and shall not be construed to affect or impair Public Law 88-290 or the authority of any entity to effect applicant or personnel actions pursuant to Public Law 88-290, Public Law 86-36, or other applicable law.

SCI ACCESS DETERMINATION AUTHORITY

3. Adjudications for access to SCI shall be made in accordance with DCID 1/14 by a Determination Authority designated by the Senior Intelligence Officer (SIO) of each entity. Access to SCI shall be denied or revoked whenever it is determined that a person does not meet the security standards provided for in DCID 1/14.

PROCEDURES

4a. Persons shall be:

(1) notified of the denial or revocation of SCI access,

(2) notified that they may request to be provided the reasons for such denial or revocation, and/or

(3) afforded an opportunity to appeal.

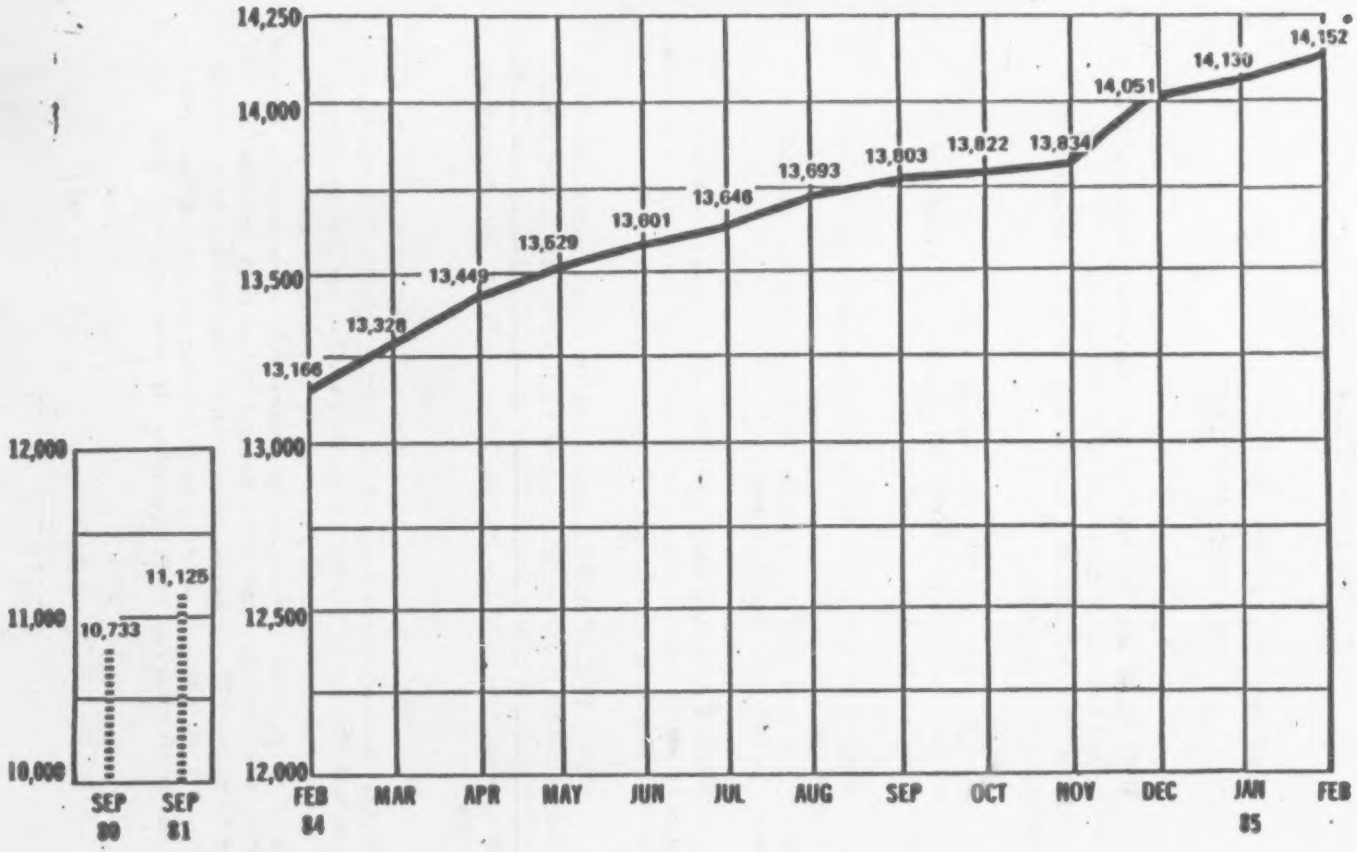
whenever the Determination Authority of any entity, in the exercise of his discretion, deems such action in any given case to be clearly consistent with the interests of the national security.

b. Any person who is given notification and afforded an opportunity to appeal pursuant to subparagraph a. above may, within 45 days of the date on which such person is notified of the reasons for denial or revocation of SCI access, submit a written appeal of that denial or revocation to the Determination Authority. The written material submitted for consideration may include any information which the person believes will assist the Determination Authority in reviewing the case.

c. After a further review of the case in the light of the written appeal, the person will be notified of the decision of the Determination Authority.

d. If the Determination Authority reaffirms a denial or revocation of access, the person may request a final review of the case. In that event, the SIO, or his designee, shall personally review the case and exercise his discretion pursuant to the provisions of DCID 1/14, and shall inform the person of his decision, which shall be final and unreviewable.

DISP FACILITIES INVENTORY



EXECUTIVE ORDER 10865

SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosures of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that those provisions and procedures recognize the interests of individuals affected thereby and provide maximum possible safeguards to protect such interest:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the armed forces of the United States, it is hereby ordered as follows:

SECTION 1. (a) The Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, and the Administrator of the Federal Aviation Agency, respectively, shall, by regulation, prescribe such specific requirements, restrictions, and other safeguards as they consider necessary to protect (1) releases of classified information to or within United States industry that relate to bidding on, or the negotiation, award, performance, or termination of, contracts with their respective agencies, and (2) other releases of classified information to or within industry that such agencies have responsibility for safeguarding. So far as possible, regulations prescribed by them under this order shall be uniform and provide for full cooperation among the agencies concerned.

(b) Under agreement between the Department of Defense and any other department or agency of the United States, including, but not limited to, those referred to in subsection (c) of this section, regulations prescribed by the Secretary of Defense under subsection (a) of this section may be extended to apply to protect releases (1) of classified information to or within United States industry that relate to bidding on, or the negotiation, award, performance, or termination of, contracts with such other department or agency, and (2) other releases of classified information to or within industry which such other department or agency has responsibility for safeguarding.

(c) When used in this order, the term "head of a department" means the Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, the Administrator of the Federal Aviation Agency, and, in sections 4 and 8, includes the Attorney General. The term "department" means the Department of State, the Department of Defense, and the Atomic Energy Commission, the National Aeronautics and Space Administration, the Federal Aviation Agency, and, in sections 4 and 8, includes the Department of Justice.

SECTION 2. An authorization for access to classified information may be granted by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an "applicant", for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.

SECTION 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked by the head of a department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of the reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the department concerned, an opportunity to appear personally before the head of the department concerned or his designee, including, but not limited to, those officials named in section 8 of this order, for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

SECTION 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.

(2) The head of the department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the department to be good and sufficient.

(b) Whenever procedures under paragraphs (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

SECTION 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the department concerned by an investigative agency pursuant to its responsibilities in connection with assisting the head of the department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered. In such instances a final determination adverse to the applicant shall be made only by the head of the department based upon his personal review of the case.

SECTION 6. Because existing law does not authorize the Department of State, the Department of Defense, or the National Aeronautics and Space Administration to subpoena witnesses, the Secretary of State, the Secretary of Defense, or the Administrator of the National Aeronautics and Space Administration, or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary or the Administrator, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination.

SECTION 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

SECTION 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a department by this order may be delegated to the

(1) Under Secretary of State or a Deputy Under Secretary of State, in the case of authority vested in the Secretary of State;

(2) Deputy Secretary of Defense or an Assistant Secretary of Defense, in the case of authority vested in the Secretary of Defense;

(3) General Manager of the Atomic Energy Commission, in the case of authority vested in the Commissioners of the Atomic Energy Commission;

(4) Deputy Administrator of the National Aeronautics and Space Administration, in the case of authority vested in the Administrator of the National Aeronautics and Space Administration;

(5) Deputy Administrator of the Federal Aviation Agency, in the case of authority vested in the Administrator of the Federal Aviation Agency; or

(6) Deputy Attorney General or an Assistant Attorney General, in the case of authority vested in the Attorney General.

SECTION 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

DWIGHT D. EISENHOWER

THE WHITE HOUSE
February 20, 1960

EXECUTIVE ORDER 10909

AMENDMENT OF EXECUTIVE ORDER NO. 10865, SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

By virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States, and as Commander in Chief of the armed forces of the United States, Executive Order No. 10865 of February 20, 1960 (25 F.R. 1583), is hereby amended as follows:

Section 1. Section 1(c) is amended to read as follows:

"(c) When used in this order, the term 'head of a department' means the Secretary of State, the Secretary of Defense, the Commissioners of the Atomic Energy Commission, the Administrator of the National Aeronautics and Space Administration, the Administrator of the Federal Aviation Agency, the head of any other department or agency of the United States with which the Department of Defense makes an agreement under subsection (b) of this section, and in sections 4 and 8, includes the Attorney General. The term 'department' means the Department of State, the Department of Defense, the Atomic Energy Commission, the National Aeronautics and Space Administration, the Federal Aviation Agency, any other department or agency of the United States with which the Department of Defense makes an agreement under subsection (b) of this section, and, in sections 4 and 8, includes the Department of Justice."

Section 2. Section 6 is amended to read as follows:

"Sec. 6. The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Administrator of the Federal Aviation Agency, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section 1(b), or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, and the proceeding involves the activity in connection with which the witness is employed, travel expenses and per diem are authorized as provided by the Standardized Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees of the executive branch of the Government or members of the armed forces of the United States not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An officer or employee of the executive branch of the Government or a member of the armed forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other department or agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination. If a person so invited is an officer or employee of the executive branch of the Government or a member of the armed forces of the United States, the head of the department or agency concerned shall cooperate in making that person available for cross-examination."

Sec. 3. Section 8 is amended by striking out the word "or" at the end of clause (5), by striking out the period at the end of clause (6) and inserting "; or" in place thereof, and by adding the following new clause at the end thereof:

"(7) the deputy of that department, or the principal assistant to the head of that department, as the case may be, in the case of authority vested in the head of a department or agency of the United States with which the Department of Defense makes an agreement under section 1(b)."

DWIGHT D. EISENHOWER

THE WHITE HOUSE

January 17, 1961

Federal Register
Vol. 47, No. 66
Tuesday, April 6, 1982

Presidential Documents

Title 3—
The President

Executive Order 12356 of April 2, 1982

National Security Information

TABLE OF CONTENTS

[FR Page]
Preamble [14874]

Part 1. Original Classification

1.1 Classification Levels [14874]
1.2 Classification Authority [14874]
1.3 Classification Categories [14875]
1.4 Duration of Classification [14876]
1.5 Identification and Markings [14877]
1.6 Limitations on Classification [14877]

Part 2. Derivative Classification

2.1 Use of Derivative Classification [14878]
2.2 Classification Guides [14878]

Part 3. Declassification and Downgrading

3.1 Declassification Authority [14878]
3.2 Transferred Information [14879]
3.3 Systematic Review for Declassification [14879]
3.4 Mandatory Review for Declassification [14879]

Part 4. Safeguarding

4.1 General Restrictions on Access [14880]
4.2 Special Access Programs [14881]
4.3 Access by Historical Researchers and Former Presidential Appointees [14881]

Part 5. Implementation and Review

5.1 Policy Direction [14881]
5.2 Information Security Oversight Office [14881]
5.3 General Responsibilities [14882]
5.4 Sanctions [14882]

Part 6. General Provisions

6.1 Definitions [14883]
6.2 General [14883]

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 *Classification Levels.*

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Attachment VII

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

Sec. 1.2 *Classification Authority.*

(a) *Top Secret.* The authority to classify information originally as Top Secret may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; and

(3) officials delegated this authority pursuant to Section 1.2(d).

(b) *Secret.* The authority to classify information originally as Secret may be exercised only by:

(1) agency heads and officials designated by the President in the Federal Register;

(2) officials with original Top Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(c) *Confidential.* The authority to classify information originally as Confidential may be exercised only by:

(1) agency heads and officials designated by the President in the Federal Register;

(2) officials with original Top Secret or Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(d) *Delegation of Original Classification Authority.*

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification author-

ity; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original classification authority by the agency head.

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.3 *Classification Categories.*

(a) Information shall be considered for classification if it concerns:

(1) military plans, weapons, or operations;

(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) foreign government information;

(4) intelligence activities (including special activities), or intelligence sources or methods;

(5) foreign relations or foreign activities of the United States;

(6) scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safeguarding nuclear materials or facilities;

(8) cryptology;

(9) a confidential source; or

(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

Sec. 1.4 *Duration of Classification.*

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

Sec. 1.5 *Identification and Markings.*

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) one of the three classification levels defined in Section 1.1;

(2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(3) the agency and office of origin; and

(4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

Sec. 1.6 *Limitations on Classification.*

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 *Use of Derivative Classification.*

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

Sec. 2.2 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1); and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

Declassification and Downgrading

Sec. 3.1 *Declassification Authority.*

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

Sec. 3.2 *Transferred Information.*

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 *Systematic Review for Declassification.*

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification o classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification o classified information pertaining to intelligence activities (including speci activities), or intelligence sources or methods.

Sec. 3.4. *Mandatory Review for Declassification.*

(a) Except as provided in Section 3.4(b), all information classified under thi Order or predecessor orders shall be subject to a review for declassificatio by the originating agency, if

(1) the request is made by a United States citizen or permanent resident alie a federal agency, or a State or local government; and

(2) the request describes the document or material containing the informatio with sufficient specificity to enable the agency to locate it with a reasonab amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

Safeguarding

Sec. 4.1 *General Restrictions on Access.*

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Sec. 4.2 *Special Access Programs.*

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

Sec. 4.3 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

(1) are engaged in historical research projects, or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Sec. 5.1 *Policy Direction.*

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2 *Information Security Oversight Office.*

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

(2) oversee agency actions to ensure compliance with this Order and implementing directives;

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Sec. 5.3 *General Responsibilities.*

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the Federal Register to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

Sec. 5.4 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5.3(a)(1) so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) Each agency head or the senior official designated under Section 5.3(a)(1) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b) (1) or (2) occurs.

Part 6

General Provisions

Sec. 6.1 *Definitions.*

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Sec. 6.2 *General.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.

Ronald Reagan

THE WHITE HOUSE,
April 2, 1982.

[FR Doc. 82-9320
Filed 4-2-82; 2:52 pm]
Billing code 3195-01-M

Editorial Note: The President's statement of Apr. 2, 1982, on signing Executive Order 12356 is printed in the *Weekly Compilation of Presidential Documents* (vol. 18, no. 13)

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * *

THOMAS J. O'BRIEN
Director
Defense Investigative Service
Department of Defense

Q. Emigres from Communist countries are prime recruiting targets of hostile intelligence operations. What can DIS do to collect background information from foreign born persons who apply for clearances?

A. The recent targets of hostile intelligence such as Cooke, Bell, Harper and Cavanaugh, have all been native born U.S. citizens. The most overriding factor has been greed and in LT Cooke's case - ideology. This is not to say, however, that we dismiss the possible threat against foreign born individuals. Because we do not know what pressures may be brought to bear, we conduct a more in-depth inquiry covering a longer span of time on immigrant aliens in the U.S. (this includes a National Agency Check with a broader base of agencies reviewed and a greater number of inquiries). In this regard, we rely on support from other U.S. Government investigative agencies who have investigative capabilities in other countries to provide what information they can to aid in the adjudicative decision.

The policy on immigrant aliens has evolved over the years in the industrial program, and we now have greater restrictions. In June 1972, the clearance of immigrant aliens policy was changed to direct that immigrant aliens would no longer be eligible for TOP SECRET clearances. The TS clearances that were in effect on that date were permitted to remain in effect until June 1974, at which time they were administratively terminated if the individual's alien status had not changed. In October 1981 our current immigrant alien policy was defined: as a general rule immigrant aliens are not to be cleared. With certified and demonstrated special expertise; however, they could be cleared to the SECRET level.

I have personally been concerned regarding the emigre problem and have discussed the situation with FBI officials. I have been assured that the Bureau provides us with all pertinent information regarding emigres that comes to their attention.

U.S. citizens (native or naturalized) are subject to the same investigative scope.

Q. Why does DIS continue to do background checks on individuals or facilities not having access to classified information as mentioned in the DOD Harper report?

A. One of the members of the Harper Commision advised us that DIS was doing clearance backgrounds on members of a labor law firm who were performing labor relations work for a cleared facility. The labor lawyers allegedly had no access to classified information. DIS takes the very rigid position that the purpose of an industrial clearance (both personnel and facility) is to allow contractor employees access to classified information in passing on classified efforts. Abuses by both Government agencies and cleared contractors do exist and we have taken an agressive approach to identifying these abuses and ensuring corrective action is implemented.

Q. Former SCT employees have told PSI that Ruby Schuler was an alcoholic to the extent that she had to leave work early due to drinking on the job. She died of cirrhosis of the liver at a relatively early age. Was DIS ever advised of this as a 6b(1) "derogatory" required under the Defense Industrial Security Manual (ISM)? Should you have been?

A. DIS was never advised of this adverse information regarding Schuler although it is our position that the contractor was obligated to report this in accordance with paragraph 6b(1), ISM.

Q. We've also been told that Ruby Schuler displayed to fellow employees "sudden wealth" -- i.e., expensive jewelry, bundles of $100 bills in a safe deposit box, a trip from Mexico with Harper on a chartered Lear Jet -- all on a secretary's salary. Was any of this reported as a 6b(1) information? Should it have been?

A. This unexplained affluence, on the part of Schuler, was not reported under the auspices of paragraph 6b(1) although it is our position, it should have been.

Q. Ruby Schuler had a Secret clearance based only on a National Agency Check. What type of background investigation, if any, would have uncovered these types of "derogatories"?

A. Obviously, the initial investigation, no matter what scope, would not uncover problems that did not exist at the time, such as unexplained affluency. However, Ruby Schuler's drinking problem might have existed at the time and may have been revealed by the Interview Oriented Background Investigation, wherein fellow employees and the subject are interviewed. More importantly, changes in a cleared individual's lifestyle and character can only be recognized by associates who are aware of indicators which reflect problems and can only be acted on where a system exists for reporting these indicators through the adverse information (6b(1)) system.

Q. Former Hughes Aircraft engineer William Bell, who was convicted of espionage for selling classified information to Polish agents, told this Subcommittee that at the time his Secret security clearance was 28 years old. Hughes testified that, had his clearance been updated, his financial and personal problems would have justified revocation of his clearance. Was Bell's clearance ever updated? If so, what reinvestigation was conducted?

A. Yes, Bell's clearance was updated in 1974 in connection with his assignment overseas. In accordance with established policy, this was a Limited Inquiry consisting of checks of the Defense Central Index of Investigations, CIA and State Department Passport Division, all of which were favorable. Additionally, Local Agency Checks were conducted in France and Switzerland, all of which were favorable.

Q. What control does DIS have regarding the volume of background investigations it is tasked to perform?

A. Generally speaking, DIS has no control over the volume of background investigations it is tasked to perform. DIS does have limited control over the number of Periodic Reinvestigations (PR) it accepts for investigation. DIS with the concurrence of DUSD(P) sets a monthly quota for PRs. The PR quota is used to balance out the DIS workload by stabilizing the pending caseload and thereby allowing DIS to maintain acceptable completion times for all personnel security investigations. Unfortunately there has been a significant increase in initial investigations and DIS has not been able to stabilize the pending caseload through the PR quotas, and case completion times have risen above acceptable levels. As a result, DIS and DUSD(P) are developing a quota system for initial investigations. A quota system for both initial investigations and PRs would allow DIS to control the volume of background investigations it is tasked to perform.

Q. Critics of DIS have said that the ability to complete background investigations in a timely fashion dictates day-to-day operations. They indicated that the emphasis to complete background investigations expeditiously is directly related to direction and pressure received from DIS headquarters. Is this contrary to DIS's mission which is to conduct background investigations to determine whether individuals are trustworthy and reliable and that their access to our national research is consistent with national security interests?

A. DIS conducts over 200,000 Personnel Security Investigations and over 900,000 National Agency Checks each year. Our policy is to conduct quality investigations in a timely manner. We are concerned about the quality and quantity. Therefore we strive to achieve a balance between quality and productivity. Feedback from our customers indicates we have been successful. In fact, we think our Interview-Oriented Background Investigation is the best in the government.

Q. Are DIS agents precluded from addressing certain issues or asking certain questions when conducting background investigations?

A DIS considers questions pertaining to religious, racial, and political matters as well as certain questions regarding personal and domestic matters to be either improper or irrelevant. As examples, without a specific reason a DIS agent would not inquire regarding an individual's:

belief in God
opposition to any or all religions
membership in a trade union
domestic problems
views on desegregation
views on racial intermarriage
frequency in voting in general or other elections
views regarding Supreme Court decisions

These questions as well as others in a similar vein are enumerated in the Agent's investigative manual and highlighted during agent basic training.

However, There may be occasions when certain of these topics may be pertinent to the personnel security standard. For example, if domestic problems center around sexual or physical abuse, they would be an appropriate target for our inquiry. Whenever a legitimate question is asked which suggests that the agent is delving into prohibited areas, the agent is instructed to briefly explain the rational for the question.

Q. When security clearances are granted based on reciprocity agreements with our allies, does DIS review the investigative and adjudicative records? Are these cases re-adjudicated in the U.S.?

A. DIS receives a security assurance, not an investigative file. The acceptance of a reciprocal security clearance with another nation is based on criteria contained in our national disclosure policy. However, if the applicant has an appreciable period of residence within the U.S., we initiate our own investigation to cover that period and perform our own adjudication.

Q. The CIA and NSA formulate corrective policy and procedures as a result of national security compromises involving their personnel. Does DIS take similar actions?

A. Yes, most recently the DoD Industrial Security Review Committee was formed to study security measures that may have been deficient with regard to the Harper case.

Q. What is your assessment of the information bank used by the FBI to respond to NACs?

A. The information bank is as good as its contributors make it. However, there is concern that it does not receive input from many local and state law enforcement entities.

Q. What are your views on hiring non-government contractors to conduct personnel security investigations?

A. I personally believe that it is an area where the government should not contract out the work.

Q. Are DIS security inspections expected or unexpected?

A. There have been recent changes in this area. We presently conduct 12% of our inspections on an unannounced basis.

Senator **Cohen**. Our next witness is Christopher Boyce, currently serving a 68-year sentence in the U.S. Penitentiary in Marion, IL. At the request of the U.S. Marshals, I ask that all persons in the hearing room remain in place, whether seated or standing, to the extent possible until the completion of Mr. Boyce's testimony.

Mr. Boyce, before you are seated, would you raise your right hand? Do you swear to tell the truth, the whole truth, and nothing but the truth, so help you God?

Mr. **Boyce**. I do.

Senator **Cohen**. Please be seated. Why don't you just begin. I know you have prepared some written testimony. I think it will be the committee's desire to have you read it in its entirety.

Mr. **Boyce**. All right.

Senator **Nunn**. Mr. Boyce, there is some water there. I think your statement is one we will all be interested in. I suggest you take your time. Take a drink of water whenever you want to.

TESTIMONY OF CHRISTOPHER J. BOYCE

Mr. **Boyce**. Mr. Chairman, several weeks ago, I spoke to the minority counsels of this subcommittee about my recollections and personal feelings concerning espionage and the Government's personnel security programs. All of my adult life, I have seen Government as a steamroller headed in my direction, a thing to be opposed at all costs. The minority counsels surprised me. During those conversations, I felt for the first time that persons from authority were speaking to me as one human being to another. As long as I can remember, I have tried to tear down that which I did not accept instead of trying to build something better. It is my hope here today that I am performing a constructive act by relating my memories. I have come here in good faith to assist this subcommittee if I can, but perhaps I need to say these things even more than you need to hear them.

In early 1975 at the age of 21, I took my first stumbling steps toward the KGB. I was a totally naive amateur. I lacked even the most rudimentary skills this subcommittee would associate with espionage. But even today, I'm still astounded at how easy the thing was to begin and, given the security system, how near impossible it was to prevent. Regardless of expensive and elaborate security systems, I suggest that espionage arrests are made mainly when beginners make artless, blundering mistakes. And such a policy that gets results primarily by picking up the pieces after a security breach instead of active individual-directed prevention is an extremely frail method on which to base security. I think that the counterintelligence elements of Government and the personnel security programs of the defense industries are missing the boat, and if you will bear with me, I will try to speak my way through to the root of the weaknesses as I see it.

On April 28, 1977, at the age of 24, I was convicted on eight counts of violating the espionage statutes and given a sentence of 40 years. My boyhood friend and co-defendant, Andrew Daulton Lee, was convicted in a separate trail on 12 counts of espionage and sentenced to life imprisonment.

In mid-1979, I was finally sent to Lompoc Prison where I was put in the incorrigible unit with hardcore convicts. One day, I was reading a book on my bunk and one of the gangs entered the cell next to me en masse and stabbed my neighbor to death. I remember watching his blood puddle out on the walkway. And not long after that, they did the same thing in exactly the same way to the man in the cell behind me. I heard all of that—the screams, the death gurgle. I was the son and nephew of former FBI agents. I did not expect to live long at Lompoc, and I decided that being shot off the prison fence was a better death than the knives. But I wasn't shot. I got away one night in January 1980. For 18 months, I remained a fugitive, despite a manhunt by the U.S. Marshals Service and the FBI.

While the Government followed leads as far away as Costa Rica, South Africa and Australia, I spent my days in Idaho and Washington State. It is a frightening life believing that every law officer in the country would be proud to put a bullet in you. I was desperate. I thought returning to prison meant my death. To live on the run, I began holding up federally insured banks. I learned about that from all the idle talk in prison. It was terribly wrong, but I never intended to harm anyone, and I didn't. All during this time, I did not hide my true identity and past from dozens of new friends in the Northwest; they were fully aware of what had gone on between the Russians and myself, and they knew that I was a fugitive.

Finally, I was turned in by a friend wanting to collect a reward, and I was arrested on August 20, 1981, in Port Angeles, WA. I pled guilty to everything, and now have 68 years instead of 40. The Government now keeps me locked in an isolation cell in Marion, IL., where I have a lot of time to think about all this in peace.

I have been told that the facts underlying the original charges against myself and Daulton are generally known by members of this subcommittee. I don't think I need to recount a long narrative of what we did Suffice it to say that from March 1975 through December 1976, I removed or photographed sizable number of classified documents from the highly secret "black vault," as they called it, of TRW, a CIA contractor in Redondo Beach, CA, and sent them on with Daulton to the KGB in Mexico City. I was able to obtain those documents through my position as a specially cleared TRW employee, working in the black vault, located in building M4. On more than a dozen occasions, I removed documents from TRW and photographed them. On approximately 6 occasions, probably more, I personally photographed documents while in the vault itself. Daulton, in turn, delivered and sold the documents to KGB agents working out of the Embassy in Mexico City. The documents pertained in part to the existence and operation of then highly secret intelligence satellites.

As an employee of TRW, I not only received confidential, secret, and top secret clearances and access to special projects, but I was also supposedly restricted by the prescribed physical security measures for classified documents. Obviously, neither the Government's clearance procedures nor the company's security procedures worked very well. In fact, the company's security procedures were a great help to me in compromising a CIA project to the Russians. There are some obvious reasons why.

Let me begin with the question of clearances. In 1975, when I sent Daulton off with the first classified documents to the Soviets, neither of us was a professional spy, to say the least. We knew as much about espionage as we did about hieroglyphics. On my part, I was not even a professional or long-standing member of the intelligence community. After dropping out of college, I went to work at TRW in July 1974. My only prior interest in the intelligence community had been one of suspicion and distrust.

At 21, in an era of Vietnam, assassinations, Chile, and Richard Nixon's resignation, I had a strong distaste for Government. I considered the CIA as, if anything, the enemy. When I came to TRW, I had no idea that my work would, in any way, involve the CIA. I got the job through what one might call the "ole boy network." My father, a former FBI agent, who then worked in security at another large defense contractor, was a friend of Mr. Regis Carr, also a former FBI agent and then manager of TRW security for top secret contracts. It was Mr. Carr who hired me.

I started at TRW as a general clerk making approximately $140 a week. I was immediately given what is known as a confidential clearance. Almost immediately, my supervisors submitted my name for receipt of a secret, and then a top secret clearance, then access to two special projects and, finally, to NSA codes. By December, all those clearances had been approved, and I was assigned to the black vault, which I subsequently learned to be one of the most secret and classified areas of work at TRW. It was only then that I learned that I would be working on a special project involving the CIA.

I was assigned with my immediate supervisor to monitor and process secret communications traffic between CIA, TRW and other CIA contacts around the world. My work included daily contact with the Intelligence Satellite Program.

In looking back, I remember being surprised that I was given such relatively free access so very quickly to those supposedly highly guarded materials. I used to sit for hours and stare into the satellite guts. It was all science fiction to me. I doubt that I would have gotten a job in the project so quickly except for my father's friendship with Mr. Carr. Unfortunately, if you accept someone because his father is a friend, it negates the entire security system.

I believe that on the day that I was hired, and prior to applying for or receiving any security clearances, the decision to place me in the vault had already been made. On that day, Mr. Carr introduced me to the director of security for a special project in building M4 as "The man you will be working for." Later I learned that this was the rhyolite project. Mr. Carr told me that I would be temporarily doing relatively routine and boring documentation for the first few months until my clearances came through for my permanent assignment.

I've been told that in other espionage cases, there were some obvious red flags of potential security violators which went unnoticed in background investigations, and by coworkers—heavy financial indebtedness; sudden affluence; alcoholism; disgruntlement.

What was my red flag? Under those indicators, probably none. I was the oldest son in a well-respected, stable, upper middle class Catholic family. My father had a fine reputation——

Senator NUNN. Mr. Chairman, at this point, let me just call attention to Mr. Bill Dougherty who is here today from California representing Mr. Boyce. We did not introduce him. Mr. Dougherty, we appreciate you being here.

Mr. DOUGHERTY. Thank you.

Mr. BOYCE. While my background investigations were underway, I heard that friends of my parents had been contacted as references. Speaking as adults, they told the investigators that I was the courteous, bright, responsible son of a good family, exactly as they were expected to say. This was the extent of the investigation, as best as I can tell.

What the investigators never sought was the Chris Boyce who moved in circles beyond the realm of parents, teachers and other adult-authority figures. To my knowledge, they never interviewed a single friend, a single peer during the entire background investigation.

Had they done so, the investigators would have interviewed a room full of disillusioned longhairs, counterculture falconers, druggie surfers, several wounded paranoid vets, pot-smoking, antiestablishment types, beaded malcontents generally, many of whom were in trouble.

In 1974, I believe that the majority of young people of my generation could not be considered politically reliable by CIA standards. I am sure you remember. Had the investigators asked any of those friends what I thought of the U.S. Government and, in particular, the CIA, I would never have gotten the job. Had they asked, they would have learned I first begun smoking pot at 16; I had experimented with a variety of other drugs along with most everyone else I knew in my age group. Had they asked, they would have learned that one of my closest friends, and later a partner in espionage, was Daulton Lee, whose records on drug charges and probation violations was, by age 22, quite extraordinary. Had Mr. Carr even bothered to question his own sons, my high school classmates, they could have easily told him far more than the Government's entire background investigation did.

From what I can tell, the Government's background investigation uncovered no substantial evidence that the CIA and Chris Boyce lived in separate Americas. They found no past arrest record, no reason to distrust me. I suggest that in an area of supposedly such grave national security considerations, that alone is not enough. The Government's background investigation also uncovered no reason to trust me. I was 21 years old. I had attended three difference colleges, and I had no idea of what I would do with myself. I had no substantial work history except school jobs. I laid concrete; I was a waiter; I had a paper route; I was a pizza cook; a janitor; a liquor store delivery boy; I harvested barely one summer—certainly nothing akin to the responsibility of handling highly classified spy satellite communications.

TRW was my first full-time permanent job. In short, I had never been tested. In my view, that should have generated some caution, especially given the tenor of the times in the early 1970's, the widespread questioning of authority, and open political dissent within my own generation. Yet, from what I can tell, TRW and the CIA never hesitated in placing me, untested and untried in their most sensitive area of employment.

I might add, that the only thing I was asked to do to get these clearances was to fill out a few forms. Although at the time my little sister was polygraphed before she went to work at 7-Eleven, I was never polygraphed. I had trouble speaking with the minority counsels about polygraphs. Should the Government be in the business of making windows into men's minds? Perhaps when a person has a security clearance, it is proper that he give up a part of himself for everybody else. I don't presume to know.

To continue, I was never given a subject interview. A year later, after I had started sending TRW/CIA documents to the KBG, I was given access to yet another special project after merely signing a few more forms. No additional background investigations were done, to my knowledge.

[At this point in the hearing, Senator Chiles withdrew from the hearing room.]

Mr. Boyce. On the question of physical security of TRW's black vault, I can answer it simply and quickly: There was none. In my view, and I believe in the eyes of my fellow workers there, security was a joke, certainly nothing to be taken seriously.

Take, for example, our project security manager, whom we regularly referred to as our "token hippie." On lunch breaks, when not drinking with us or others at the local bars, he would often be skateboarding around the neighborhood. Sometimes he returned the worse for wear, with bruises and torn pants. On one occasion, he told me he wanted the security atmosphere in M4 to be as unintrusive as that on a college campus.

I can recall one incident where he did take an especially active role in security. The M4 coffee fund for employees was found consistently short. The old night janitor was suspected of theft. One evening, the project security manager phoned me in the vault and told me that I was to come upstairs after work to help him "catch a thief." We then drilled a hole in an office wall so that he could watch the coffee fund without being seen. For the rest of the evening the project security manager sat in the dark peering through a hole, eventually catching the janitor pinching a few quarters. When the "surveillance" began, I went back down to the vault and made myself a drink, wondering at the lunacy of it all. The system could catch a janitor stealing coffee money, but it was incapable of hindering me in any way from passing the entire project to Daulton and on to the KGB.

I suppose most people view security regulations as something that should be held in awe by employees. That was clearly not the case at TRW. A number of employees made phony security badges as pranks. My immediate supervisor once made a security badge with a chimpanzee's face on it, and to everyone's amusement, used it to come in and out of the building.

The security identification badges themselves were not strictly accounted for. There were boxes of old badges that employees had previously used that were not destroyed for months at a time. These could have been used for improper entry. Prior to coming to the black vault, I worked in badges for a while. There was no accountability over the materials used in the manufacturing of identification. I could have made a badge, an ID for anyone, giving them access to a number of classfied areas.

On one occasion in late 1974, before being sent to the Rhyolite project, a special project manager arrived at Badge and ID accompanied by an outside consultant. I refused to make badges and identification for the consultant because he was not accompanied by the proper clearance paperwork. The special project manager swore revenge and she later got it by having me temporarily transferred out of security.

Aside from badges, there was almost no supervision over access to the building and the vault. Although my comings and goings at building M4 were logged by the security guards, there was nothing to stop me from entering at any time during the day or night. On occasion, I returned to the vault late at night without being questioned or even raising suspicion. There was simply no questioning on after-hours access as long as one mentioned any plausible excuse in passing, such as, "I forgot my tennis racket." Once inside, there was no monitoring of my after-hour activities in the vault. None of the security guards who would log my entrance or inspect the premises had authorized access to the black vault.

[At this point in the hearing, Senator Chiles entered the hearing room.]

Mr. BOYCE. During some of these after-hour visits, I photographed and removed documents. For a while, I used to come to work at 4 a.m. to process the teletype traffic from Langley and then shut down and lock up at 5:30 a.m. in order to hunt jackrabbits with my Harris Hawk at sunrise. I would then return to work around 7:30 a.m. and reopen the vault. No one questioned this. I could come and go whenever I wanted. I remember laughing about this with a girl I knew who was a bank teller. She used to tell me that Security Pacific would never allow their employees to open and enter their vaults at will unsupervised at any time.

Controls on access beyond the communications vault area were hardly much better. As part of my courier duties, I made deliveries to the CIA facility. Although I had no clearances or authorization to do so, on occasion, I wandered into their code room. Once I recall talking to a female employee inside the vault there. On a clipboard hanging on the wall beside her was a list of the station codes on their circuit. Because I was naturally curious about everything that went on there, I began to note all the handles. She caught me reading it, paused to flip the board over and just smiled. I do recall that one employee did ask me to leave because I was unauthorized.

Within the TRW vault, management had effectively compartmentalized security away. By making the vault such a highly secret area, those of us inside had been given, in effect, total autonomy. We worked under our own set of rules, or more accurately, lack of rules. We brought in an uncleared company locksmith and altered the numbers on the vault tumblers by half clicks to prevent unauthorized access by our superiors. We did not want them trespassing on our private preserve. We regularly partied and boozed it up during the working hours within the vault. Bacardi 151 was usually stored behind the crypto machines.

Under security regulations, we were required to destroy the code cards for the machines daily in a destruction blender. We chose instead to throw the cards toward, but not necessarily in, canvas bags in the corner. We used the code destruction blender for making banana daiquiris and mai-tais. Although only about eight people had authorized clearances to the vault, often many noncleared members of our club, so to speak, would be in the vault for libations. On occasion, the project security manager would join us for a drink on the house.

Part of our information duties included frequent runs to the liquor store with orders from various employees throughout the building. We used the satchel for classified material as a cover to bring in their peppermint schnapps, rum, Harvey Wallbanger mix, what have you, along with our stout malt, back into M4. In doing so, I sometimes used the satchel to take classified documents out. To return the documents, I used packages, potted plants, and camera cases. Packages and briefcases were never searched by the guards.

On one occasion, I needed to return a rather large ream of documents—about this big [indicating]—that I had taken out earlier in the satchel on a Rhyolite beer run. I went to a floral shop and bought two huge clay pots about 2 feet tall. I put the ream of documents in one after wrapping them in plastic, covered it with dirt and stuck bushy plants in both pots. I brought one of the plants into the building myself and asked the security guard to carry the plant holding the documents back into the building. He obliged.

A more severe security breach regularly entered our vault over the encrypted teletype link from Langley. Routinely, we would receive from the CIA communications operators misdirected TWX's on other contractors' projects. We were not cleared for these projects, and there was no accountability for misdirected TWX's we received other than a lackadaisical request to destroy tapes from the Langley communication operators.

To briefly return to badges and identification, the camera and film used to photograph employees for their picture identification were stored in one of the black vault safes on a shelf directly beneath the NSA crypto codes. It always struck me as both odd, but still typical at TRW, that objects such as these would be stored together.

I remember only two Government inspections in the vault during the entire time I was there. It amazed me that even though we were using all this highly secret equipment that belonged to the Government, the Government wasn't even around to oversee it. As for TRW's own security, Mr. Carr, the security director, could not take two steps toward the vault without our knowing about it in advance. The security guards always warned us in plenty of time concerning his movements. As a result, as far as I can tell, Mr. Carr was completely unaware of the security breaches in the vault. He gave his orders from inside a bureaucratic cloud.

I distinctly remember one of two Government inspections. The code cards for the crypto machines came in checkbook-style binders sealed in clear plastic envelopes. The envelopes were to be unsealed and binders removed only at the beginning of the month they were to be used. We were given books of these codes, sometimes 5 months in advance of their data use, despite obvious security risks.

I was amazed that the NSA would let half a year's worth of their codes sit any where out of their possession.

At the time of the inspection, I had been unsealing some of these future codes, removing them and photographing them. I would reseal the plastic with the heat from an iron or with glue and then replace them in the vault. They were all packaged in established official manner. The inspector came across one code binder that I had replaced upside down and face down and then resealed. Once tampered with, the plastic envelopes never looked quite the same, despite my botched efforts at resealing them. He noticed it, looked puzzled, but instead complained about some other relatively insignificant missing item—one that no one could remember. He had looked closely at the displaced code card binder, but chose to pass over the broken seal.

Document control itself was poorly supervised. It was one of my tasks to take the TWX's and other messages to our reproduction center. From there, I would distribute copies to various authorized recipients in TRW. On numerous occasions, I would see different employees later reviewing these classified documents even though they were not cleared for access to them. At times, employees would ask me for additional copies of these classified documents given them since they couldn't find or had lost their assigned copies.

My experiences at TRW have caused me to come to certain conclusions about personnel security. I know that a number of changes have been made in the way the Government conducts background investigations that supposedly alert the investigators to potential security risks. I have been told that there is now greater emphasis on peer and background investigations. This was a basic reform if it has stuck.

Friends and parents simply could not give a true insight into what made Christopher Boyce tick. As I said before, if this had been done, I believe I would have never gotten the job in the first place.

Second, I should have been interviewed in great detail regarding my lifestyle and attitudes. I was never questioned about these points which seem to me to be important indicators for future security breaches. Had I been interviewed in this manner, I also believe I would never have been assigned to that sensitive position.

Third, I know that if I had been polygraphed solely on attitudes toward the Government, and the CIA, or even marijuana use, I probably never would have been considered for the job, but then neither would most of the friends I grew up with.

There are also a number of changes in security procedures that would have deterred my brazen act and also greatly increased my chances of getting caught. Although these suggestions might not stop the professional spy, they would certainly have affected amateurs like myself.

First, supervision over special projects, such as the one I was involved with, must be strengthened, expecially supervision over the security sections of the special projects. There was little, if any, outside influence over our day-to-day activities. We were project security and we viewed security as a joke because we could easily circumvent it by our insulation from the usual management controls.

What little security we saw was ineffective and incompetent. If we had been strictly supervised, perhaps I would have thought twice before acting as I did. Instead, I decided that the intelligence community was a great bumbling, bluffing deception.

Second, a policy of inspecting every parcel, briefcase, and package going into and out of the building, such as M4, should be implemented. Although this in and of itself would not have prevented me from concealing material on my person, it would have increased my awareness of security as well as my chances of getting caught.

Third, metal detectors should be installed in buildings such as M4 where there are highly secret projects. Such devices might have prevented me from bringing the camera that Daulton gave me repeatedly in and out of the project area.

Fourth, if there had been encoding devices on the classified documents that could be monitored at building exits, I would never have attempted to take the actual documents out. I am aware of similar devices on library books and items of merchandise that sound alarms if one attempts to remove them.

Fifth, a policy of limited polygraph examinations at the time of termination of employment on questions of unauthorized disclosure should be implemented. This policy should be explained to the applicant for employment at the time of hiring. He should be reminded of this policy throughout employment. If I had known this, I would never have considered an act of espionage. Contrary to assurances to me by the KGB officer in Mexico City that they had ways to beat the polygraph, I knew that I could not pass a polygraph and greatly feared it. The same fear heightened my resolve never to accept direct employment with the CIA, although on two separate occasions, it was offered.

This policy, distasteful as it is, should be considered one of the best deterrents to those toying with the thought of espionage.

Sixth, for the same reasons, I think that the limited use of the polygraph at the time of an employee's update investigation would heighten the fear of being caught sooner in a case such as mine, but fear alone cannot achieve security.

Seventh, the number and scope of onsite investigations by the Government should be increased.

[At this point in the hearing, Senator Chiles withdrew from the hearing room.]

Mr. Boyce. Both of the two inspections I recall at TRW appeared to be pro forma, just requiring us to show the inspector that we had certain items on their checklist. Never once were we questioned on knowledge of, or compliance with, security procedures. Never once, as I recall, were questions asked concerning our very cluttered workplace. Never once were questions asked on destruction of old ciphers or other classified materials.

Eighth, I recommend some system of anonymous complaints concerning security breaches that would be directed to the Government and not to the company. If I had seen posters on some sort of hotline system operating within the company, it would have given me pause to consider what I was doing. It would not only have deterred espionage, but it would have deterred everything else.

All of this brings me to another point I would like to raise. I am convinced from my own experiences that what I say now is by far the most useful contribution that I can make to this subcommittee's study of personnel security. While I think these security regulations you review are important to maintain the integrity of the Government, I believe that they are next to worthless if each of the 4 million Americans with security clearances do not have a grasp of how espionage would affect them personally.

No matter what the security procedures are devised, if a man built it, another man can circumvent it, and usually in the most simple way. At best, physical security can only make things tougher. The increase of espionage that you are experiencing will not be a passing phase unless popular myths about espionage are debunked for the fraud they are.

I think even in these responsible times, that if not carefully monitored, the intelligence community of any Western nation can be potentially a threat to an open society. But there is nothing potential about the KBG. That state apparatus not only threatens every open society, but it crushes open societies. That is the distinction that I could not see at rebellious 21, and it is a distinction which Americans must see.

The security organizations of both sides spy and engage in clandestine tactics. And in Mr. Gorbachev's new age of Camelot at the Kremlin, it will perhaps be easier for naive Americans to rationalize away the distinction between the restrained secrecy that defends them and the stealthy menace that seeks to deceive them.

By your own estimates, there are at least 500 KGB agents in the United States. And, Senators, I respectfully suggest that the overwhelming majority of the 4 million Americans with security clearances are extremely naive in their conceptions of espionage. That is the root of your problem.

When I was at TRW, I and several hundred other relatively fresh employees were given a group talk on the perils of espionage. A clean-cut all-American type addressed us from the podium. Here I sat with the KGB monkey already on my back, surrounded by all these young people who were being fed totally inaccurate and inappropriate descriptions of espionage. They were given the impression that espionage was some exotic, glamorous escapade, handsome Slav spies would seduce young American secretaries on their vacations in Brussels and bend them into secret agents for the KGB. That type of approach to preventing espionage was and is disastrous. That was just what all those bored, young secretaries around me were dying to hear.

It was surreal. A Government spokesman already accepted by everyone as competent stood there entertaining all those naive, impressionable youngsters around me with tales of secret adventure, intrigue, huge payoffs, exotic weaponry, seduction, poisons, hair-raising risks, deadly gadgetry. It was a whole potpourri of James Bond lunacy, when, in fact, almost everything he said was totally foreign to what was actually happening to me.

Where was the despair? Where were the sweaty palms and shakey hands? This man said nothing about having to wake up in the morning with the gut-gripping fear before steeling yourself once again for the ordeal of going back into that vault. How could these very ordinary young people not think that here was a panacea that could lift them out of the monotony of their everyday lives, even if it was only in their fantasies?

None of them knew, as I did, that there was no excitement; there was no thrill. There was only depression and a hopeless enslavement to an inhuman, uncaring foreign bureaucracy. I hadn't made myself count for something. I had made my freedom count for nothing.

As we sit here a half dozen, perhaps dozen, perhaps more Americans are operatives of the KGB. Perhaps some of them have been in place for years. I tell you that none of them are happy men or women.

And I would suspect that there are hundreds of other Americans out of the 4 million with security clearances who have given serious thought to espionage. Those are the people that you must seek out and reach with the truth. It is infinitely better for you to make the extra effort to ensure that your personnel understand beyond a shadow of a doubt how espionage wounds a man than for more and more of them to find out for themselves. No American who has gone to the KGB has not come to regret it.

For whatever reason a person begins his involvement, a week after the folly begins, the original intent and purpose becomes lost in the ignominy of the ongoing nightmare. Be it to give your life meaning or to make a political statement, be it to seek adventure, or to pay delinquent alimony, be it for whatever reason, see a lawyer or a psychiatrist or a priest or even a reporter, but don't see a KGB agent. This is a solution to nothing.

I only wish, Senators, that before more Americans take that irreversible step, that they could know what I now know, that they are bringing down upon themselves heartache more heavy than a mountain.

Senator COHEN. Mr. Boyce, I want to thank you for what I consider to be one of the most powerful and, I would dare say, poignant statements to have ever been made before this committee or any other committee in the U.S. Senate or Congress. And, what you say about the KGB, I think, has to ring true. Your, perhaps, most telling statement is the KGB not only threatens an open society, but it crushes an open society, and we are at times rather hopelessly naive about the designs and capability.

Mr. BOYCE. Yes, sir.

Senator COHEN. I tell you from personal experience from chairing a hearing not too long ago dealing with our military capabilities, a Soviet KBG agent sat and listened to an open discussion of our naval tactics. I found this absurd. Immediately upon discovery, I closed the meeting down. But we are terribly naive about their presence and their capability and their designs and I think your statement is particularly an important one.

[At this point in the hearing, Senator Gore withdrew from the hearing room.]

Senator COHEN. I might also say, Senator Nunn, Senator Roth and I all serve on the Intelligence Committee.

Mr. BOYCE. Yes, sir.

Senator COHEN. I couldn't help but listen to your testimony and think at times we are living in the theater of the absurd, and that we go through security precautions, we don't talk on telephones, we don't talk in our offices, we don't even talk on elevators to our staffs because we don't dare risk having this information disclosed. And then you describe a situation in which it's almost as if a marginal wall has been constructed, the other side of which are those who are the keepers of secrets.

Mr. BOYCE. Yes, sir.

Senator COHEN. I know that in talking to the staff, you really have focused upon this notion of how naive Americans really are. This naivety, you say is perpetuated by the espionage and spy novels and glorification of the spy itself.

Let me tell you something, there is no novelist that I am aware of who has a fertile enough imagination to have constructed the scenario that you have—token hippies, janitors stealing coffee money, phone security badges being produced by employees, after-hours access to get your tennis racket, altering combination locks so your superiors could not enter the vault that you were given custody of for the time being, parties and booze being consumed in the vault itself and on and on, to Bacardi rum being stored behind the crypto machines. No novelist that I am aware would have imagination enough to have constructed that.

I suspect there are representatives from TRW here, and I am aware of a number of precautions they have taken since that time. I would hope one benefit of this particular hearing would be that, not only TRW, but every single industry representative here understands what has happened and what cannot be allowed to take place in the future. This sort of laxity, which, in my judgment, is tantamount to criminal activity, cannot be tolerated if we are going to maintain any sort of secrets in our society.

So I want to thank you for that and perhaps call upon you to expand upon this glorification of becoming an agent for the KGB. I know you mentioned to the staff that the book, "The Falcon and the Snowman" itself glamorized what really happened. The movie version, you have said, also focused upon the comical or the absurd rather than the serious, substantive aspect of what happened.

Mr. BOYCE. Can I show you something that I brought with me? I was just watching television a while ago and saw this program on so I watched it for laughs. It's called, "Secret Weapons." It was on about a month ago. You see, I think there is a whole generation of Americans who are coming on who have a view of espionage that is just totally false from the reality of espionage, and I think the entertainment industry really pushes that along.

You take a program like this "Secret Weapons," starring Linda Hamilton as the KBG terminator. There she is in bed, very gorgeous gal. It says, "A Russian spy in love with an American. In 23 seconds, she must decide her lover or her life." And it goes on to say the secret weapons are young Russian women recruited in training by the KGB to seduce targeted Americans.

It makes espionage into something that it isn't. Does anybody really think, anybody with any knowledge really think that's espionage? All the people watching it believe that—I mean, the Marine Guards at the White House would be interested in this. It's disinformation—it's misinformation really; it is not disinformation. If it was disinformation, the Russians would be putting it out.

When people see this, they get a totally wrong view of what espionage is. This had a happy ending. Even the KGB control agent who was setting these Russian women up as call girls, even he turned out to be a nice guy who told this Linda Hamilton, "yeah, well, go to America and be happy with your American lover." [Laughter.] There's another program that's really garbage on television. It's called "Scarecrow and Mrs. King."

Senator COHEN. I am not sure you should start listing all the programs. [Laughter.] I think we got the message. Could I perhaps turn to questions dealing with your meeting with the Soviet agents? You met with them on one occasion, did you not, in Mexico City?

Mr. BOYCE. Yes.

Senator COHEN. During that meeting, did they ask you about approaching some other employees at TRW? Can you tell us what took place at that time?

Mr. BOYCE. Well, from the TWX's that they already received, they already had a knowledge of people in the project. What they wanted was a list of everyone that was in the project, and they wanted me to tell them different things about these people that could be exploited—financial problems, alcohol problems, sex problems, who was going on vacation where and when, to which countries, and just things that they could use to put hooks into people and exploit them—that is what Boris was after.

I did not give him that, but that's what he wanted.

Senator COHEN. By the time you met with the Soviet agents, you had already decided to leave TRW; is that right?

Mr. BOYCE. Yes, sir.

Senator COHEN. Did they have any plans for you for the future?

Mr. BOYCE. Well, I told them, when I went down there, I told them I was leaving and that was over, and something had to be done about Daulton. Not that he had to be hurt or anything, but that he was totally out of control and wasn't there something they could say to him or do. And I told Boris that I was going back to school. And his eyes lit up. He thought that was a great idea. He was talking about a long-term type of thing. He wasn't at all disappointed that I was leaving TRW. He was thinking in terms of not next year or the year after that, but the 20, 30 years down the road of the same relationship continuing on and on. He was talking in terms of the State Department.

Senator COHEN. Did he suggest to you that you might go on to school and study international relations?

Mr. BOYCE. Yes.

Senator COHEN. And then end up in the State Department or some other Government agency?

Mr. BOYCE. Or some other branch of the Government.

Senator COHEN. Hopefully not Congress. Did that come up?

Mr. BOYCE. No.

Senator COHEN. Mr. Boyce, the security briefing you described occurred several years ago. The question I have is, do you have any evidence that employees today still glamorize or see this espionage in some sort of glamorized light?

Mr. BOYCE. Well, I received a lot of letters from young women not just who are thrilled about books and movies and newspaper articles and thrilled about espionage, but I get letters from young ladies with security clearances after they have a security briefing at one of the aerospace companies or one of the other defense companies where they talk about espionage, and where they happen to mention me. These young ladies send me letters telling me they are thrilled at the thought of espionage, interested in my case and they want to be secret pen pals. I don't have any secret pen pals because the warden reads everything that I read.

It would seem to me that if a young woman goes to a security briefing at one of your aerospace companies and is thrilled by espionage and wants to communicate with me about it, it seems to me that they are giving the same type of security briefings now that they were then.

Senator COHEN. You mentioned in listing your seven or eight recommendations, which I think made a great deal of sense, frankly, the need for polygraph at termination of employment. The question arose in my mind, why at the termination of employment as opposed to beginning of employment? For example, suppose you decided to leave TRW, and you were contacted by the Soviet agents; who knew you were going to leave. At that point TRW had a polygraph exam you had to take. Wouldn't the normal recommendation to you by a Soviet agent be, "Gee, Christopher, why don't you stay on for a while; let's not think about terminating for the next 20 years and think about moving up at TRW"?

Mr. BOYCE. I don't necessarily think everybody should go out and be made to take polygraphs. In certain positions, if you had the polygraph in the beginning, you're inhibited; you know what it is. You know you can never get out of that job without taking a polygraph, and in the meantime, there are going to be, every several years, the update investigations when polygraphs should take place.

It seems to me Thomas Jefferson would be rolling over in his grave, the Government giving people polygraphs. All I can say, it is something you really thought about, distasteful as they are.

Senator COHEN. What about the individual who was your supervisor at TRW? Do you know whether he is still with TRW?

Mr. BOYCE. No; before I left TRW, he was transferred to another special project with a heavy security clearance in another company, but I don't know where he is now, Senator.

Senator COHEN. Are you aware of the changes that were made at TRW? Can you comment in your judgment whether or not it would help deter the kind of activity you engaged in?

Mr. BOYCE. Well, Senator, one thing I recall, they talked about keeping two comm operators in the vault at all times whenever it is open. Now, it would seem to me that some upper bureaucrat in the Government says, there's going to be two comm operators in the vault at all times, but I certainly wouldn't believe that in all your vaults there's two comm operators at all times. By the time that order goes down through the bureaucracy and gets down to the trenches to the people who are actually doing the work, this is just another piece of paper.

People are human; they want to go have a cup of coffee; they want to talk to their girlfriend; have to go to the bathroom; go to the doctors. You may make those regulations but when they are applied at the lower levels like that, it's just so much paper.

Senator COHEN. Senator Nunn?

Senator NUNN. I share Senator Cohen's sentiments in terms of the importance of your testimony, Mr. Boyce. We are grateful to you for being here today. I know that many things you said here are not things you enjoy saying. They are not things we enjoy hearing. I think it's a personal tragedy for you and a tragedy for our country. Especially important is the distinction you made so well in your statement: that the dangers inherent in intelligence in a free country are potential dangers, whereas in the Soviet Union, a totalitarian society, those dangers are not potential, they are real. I know you came through an era where it was very difficult for young people, not just for you, but for many other young people to understand that distinction. Most young people did not go to the extremes that you did, and did not damage the country. I think we have to keep that in mind, also.

But what you have done here today, I hope, will in part help repair some of that damage by discouraging other young people today and people of every age who are responsible to this country for classified information. Your testimony will help them understand the pain and the agony and the suffering and the anxiety, the mental turmoil that espionage involves and not, as you said, just the glamour part of it which in many cases does not exist at all.

I am interested in pursuing a little bit what you would do if you were briefing a group of young people who were cleared for classified material, if you were a security officer, let's say, at TRW. If you had, let's say, 15 or 20 young people in a room that had just been brought into the plant and were going to be dealing with classified information—I think you pretty much made clear the kind of information you feel is exaggerated and not helpful—what kind of information would you give them, in terms of protecting this Nation's secrets?

Mr. BOYCE. Well, I wouldn't detract from what they are already told in the area of what they can do to the Government. They know that; by extension they should know what they can do to the people. People deal with things on personal levels, and a man should know what it would mean to him, what kind of life he would have in a future after that. It's just so totally unattractive a thing to be into that you're never going to get away from and it's never going to end, and it will just drag on and on, that's the type of thing people should be told.

Senator NUNN. You would tell them about the agony of your own experience?

Mr. BOYCE. I would tell them they are going to regret it; that there just isn't anything about it like the way it's pictured in the public's mind. That is just not what espionage is. [Witness conferring with counsel.]

There is no exit from it. I would have—when it was over, as far as Daulton was concerned in Mexico City, Senator, I could have left; I could have been gone. But go where? For what? And then have what kind of life after that? And even if you do flee to the

Soviet Union, you're cut off from all you family and friends—who wants to live there?

I don't know what else I would tell—what people should be told, other than how it would affect them as individuals and if a person knew that, that makes all the difference in the world.

Senator NUNN. I believe that you have some photographs there. Could you share those with us and tell us what they are? Perhaps you can hold them where we can see them here. Staff or one of the marshals perhaps could assist in showing us the photographs. If you would hold it up and explain each one, I would appreciate it.

Mr. BOYCE. Well, this is the work area, the front——

Senator NUNN [interposing]. You might want to show it where the cameras can also pick it up.

Mr. BOYCE. This is the front of the work area of the communications side of security. This in the background is the black vault.

Senator NUNN. That is the black door we see back there?

Mr. BOYCE. Yes, sir.

Senator NUNN. Maybe one of the marshals could bring it up here.

Mr. BOYCE. This is the K.W. crypto machines themselves. One thing I would like to say about the pictures is, they were taken after I left there, and this place has really been cleaned up. These pictures are not what it looked like when I was there. Big sign on the wall, "This area is for visitors only," this is after I was arrested that they put that in there. This is the K.W.-7 and this is the inside of the vault.

Senator NUNN. Hold it up there.

Mr. BOYCE. There are the K.W.'s and they fit——

Senator NUNN [interposing]. K.W. being?

Mr. BOYCE. The encrypting device itself. These keys here opening—the code cards are put there and closed. These K.W.'s are in these large machines that I just showed you.

This picture is inside the vault itself, the log desk where all the incoming, outgoing traffic was logged and the door of the vault is over here. It was on this desk that I did a lot of photographing.

Five here is the outgoing TWX desk, where the messages were sent back and forth. In the background here you can see these reams of paper that are fed into these telex machines here. It was a ream such as that, only larger, about this bit, about this long [indicating] that I brought back into the facility in a potted plant.

Senator NUNN. How did you get all that in a potted plant? That must have been a pretty big plant.

Mr. BOYCE. The plant went up another 3 or 4 feet.

Senator NUNN. Is that a routine-type thing, people taking plants in and out of that area?

Mr. BOYCE. There were plants all over the place, and nobody thought to look in a pot.

Senator NUNN. Is that the one the guard helped you to bring back in?

Mr. BOYCE. Yes; these are the telex machines inside the vault—six. This is all different from when I was there. All these shelves up here were loaded down with—"unregistered" is not the word—but unaccounted-for documents on all these shelves that we just had reference to and all our tapes.

Senator NUNN. Turn it this way.

Mr. BOYCE. That is the inside of the vault.

Senator NUNN. How was it when you were there?

Mr. BOYCE. It was just a mess. Behind this is where the booze was. Documents coming out of the top here. Everything should be stamped and you should know where every document is and accounted for. We didn't; we did whatever was convenient.

This is another picture in the black vault of the telex machines. In this picture, you can see here on the wall where my superior, Chris Sherman, banked an over-the-hand shot with a half-empty wine bottle toward the document refuse canvas bag and where the wine bottle broke against the wall.

Senator NUNN. That is the staining there?

Mr. BOYCE. Yeah.

Senator NUNN. Mr. Chairman, I would like each of those pictures be made exhibits.

Senator COHEN. Without objection, they will be included.

[The pictures referred to were marked "Exhibits Nos. 19 through 25" and may be found on pp. 1335-1341.]

Senator NUNN. They have been looked at and they do not contain classified information.

Mr. Boyce, you mentioned that the KGB said they had ways of beating the polygraph. When was that that they told you that? Was that on the visit to Mexico?

[At this point in the hearing, Senator Chiles entered the hearing room.]

Mr. BOYCE. Yes, sir.

Senator NUNN. Had you mentioned polygraph to them, or what brought that up?

Mr. BOYCE. Well, they were making all these suggestions. I was saying, talking about polygraphs, my fear and how that would be impossible because I was pretty sure the State Department uses polygraphs. The told me: "Oh, that's no problem, we have ways of having the person pass polygraphs." I didn't go into it with them at that point.

Senator NUNN. They never did give you instructions for that?

Mr. BOYCE. No.

Senator NUNN. They said they had ways of beating polygraphs?

Mr. BOYCE. Future option.

Senator NUNN. When you were meeting with the KGB people in Mexico, did they ask you to recruit any of your fellow employees?

Mr. BOYCE. Well, sir, they wanted to know all the different people.

Senator NUNN. What kind of information did they ask you for?

Mr. BOYCE. Well, they were interested in background investigations on everyone in there. Who was a homosexual; who has a problem with his wife; who is a drunk—any type of hangup that anybody had, they wanted to know about as a future exploitation-type thing.

Senator NUNN. Does that indicate to you pretty clearly that those were kinds of personnel interviews ought to be directed toward, whether they are initial interviews or whether they are renewal interviews on clearances, any kind of personal problem?

Mr. Boyce. Well, yeah, I think you definitely should, Senator. You mean with background investigations before?

Senator Nunn. Yes.

Mr. Boyce. Yes, sir; I would think that the background investigation that was done on me, although thousands of dollars was spent on it, was a joke.

Senator Nunn. Were you asked those kinds of questions before you were hired?

Mr. Boyce. No.

Senator Nunn. You were never asked whether you had a drinking problem?

Mr. Boyce. No, nothing like that. The only think I talked about with the special project manager before I actually went to work, the only think I talked about was my Harris Hawk.

Senator Nunn. Were you ever asked whether you used drugs? I believe you indicated you were not asked that question.

Mr. Boyce. Never directly by anyone. The question was, Senator, have you ever been arrested for it. I don't recall being asked if I ever—the question have you ever been arrested, no, but there are a lot of people who aren't arrested who are into drugs.

Senator Nunn. If you had been asked those questions, would you have been truthful in your answers at that stage before you had been involved?

Mr. Boyce. If there had been an in-depth, background-type investigation on me with a lot of questions like that, I don't think I would have wanted the job. I think I would have said, that's OK. The only thing else I want—do you mind if I say something about background investigations?

Senator Nunn. Go ahead.

Mr. Boyce. I read a study—I can't quote it—a while ago a sociologist wrote, and he did a study on Americans, and he found that the average American tells three good lies a day, and when you send people out on these investigations to go out and talk to friends and associates about someone, well, you don't want to say anything bad about your friends to an investigator from the United States. If you are going to, you are not that person's friend to begin with. So your investigations have to be thorough. They sure didn't investigate me.

Senator Nunn. If they had questioned your friends and your peers, do you believe your friends and peers would have given investigators information that would have led to the denial of your security clearance?

Mr. Boyce. Senator, I think all they had to do was look at my friends and peers. [Laughter.] I am not being facetious.

Senator Nunn. They didn't have to ask them questions; just look at the atmosphere.

Mr. Boyce. Yes, sir.

Senator Cohen. Let me follow up on one question. You hesitated a moment when Senator Nunn asked you whether you had been asked any questions about drug use or anything else, and whether you would have told the truth at that time. You hesitated a bit. I guess the question that comes to my mind is, if you had known they had done a thorough background check on you, would you have been less likely to lie about it? What if they asked, for example, did you ever use drugs, and you lied and said no, and they had a piece or paper that said they talked to several of your friends, or quasi-friends who said at a party on thus and such, that you, in fact, were using drugs?

If to the extent they had done a thorough check, would you have been more likely to tell them the truth than lie about it?

Mr. **Boyce**. Yes.

Seantor **Cohen**. Senator Nunn.

Senator **Nunn**. One other question. You mentioned glamorization, television, all of that. You mentioned several programs you though fit into that category. About the movie "The Falcon and the Snowman," how do you describe that, or have you seen it?

Mr. **Boyce**. Yes, sir; Timothy Hutton brought that in and I watched it with him and the warden. I know a little bit about how that was put together. Some of the fights behind it. When they make a movie about espionage, people sit down and want to watch, the producers want them to be entertained, and when they compress 2 years into 2 hours, they want to take the highlights and whatever would be exciting or out of the ordinary, and they cram it down into 2 hours instead of dwelling on the day-to-day agony of going through it.

I could relate to that film because when they got to the editing process of that film, Tim Hutton put his foot down to slow as much as he could the producer's Hollywood blitz of the film, to make it into a show-biz-type movie.

When I finished watching that film, I walked away from it feeling like I had been dragged 5 miles behind a horse. I don't think that anybody who went and saw that film walked out of there wanting to become a KGB agent. Perhaps that might have hurt the film. Perhaps the film won't do as well because it wasn't all excitement. I hope it wasn't. It didn't appear to be to me. Because I was watching it, I could feel the pain of the film. Perhaps other people couldn't. I could relate to what was there.

Senator **Nunn**. You believe that film did discourage in its final message——

Mr. **Boyce** [interposing]. Well, I hope it does. As much as it does, as much as people can look at that film and not want to become an agent of the KGB or even get into espionage, a lot of that is due to Timothy Hutton putting his feet down at the editing process and really threatening to disclaim the whole thing and walk away from it.

Senator **Cohen**. Mr. Boyce, if I might interject, you are talking to a particularly sensitive audience here who know what it is like to have their words perhaps gathered over a period of 10, 20 years reduced to a 10-second segment on the evening news. Senator Chiles?

Senator **Chiles**. Did the film still portray the situation, the anxiety that you actually felt, or whatever feelings you had?

Mr. **Boyce**. The parts that related to me did in some areas that Hutton was able to get it across. I was satisfied he at least made the effort, and what's there is there because he fought to put it there, otherwise there is no telling where the producers could have taken that thing. I don't know.

Senator CHILES. I don't want to put any words into your mouth but it sounds like being a spy is the most glamorous thing in the world.

Mr. BOYCE. It's pretty dirty business, actually. People just don't understand what it is; they just don't know what a person goes through day to day in that sort of thing. It's not what you see on television.

Senator CHILES. Can you tell me, approximately at what stage you felt the hook?

Mr. BOYCE. As soon as he came back, as soon as he was back. It just totally envelopes your life and you just pretty much stop thinking of anything else. It concentrates you on that. And any good intentions that you had in the beginning in doing what you were doing just become totally suppressed in the nightmare that is going on right around you as the thing proceeds.

Senator CHILES. So there was a totally different feeling from there, from where it started, or what you thought it would be like, or what you though you were doing?

Mr. BOYCE. It is so totally different than what I thought it was going to be like. It is even hard to explain with words, sir. Anybody that has ever got into espionage knows exactly what I am talking about 1 week later and regrets it.

Senator CHILES. Thank you.

Senator COHEN. Mr. Boyce, I want to thank you for your testimony today. There is only one other thing I would add. I know you are speaking from the heart, and your own personal experience about the horror and the no-exit sign that is hung on the inside of your own mind once you take this step into a foreign intelligence service like the KGB. And you recommend that that be stressed during these briefings.

Mr. BOYCE. Yes, sir.

Senator COHEN. To the aerospace industry. Another aspect has to be mentioned. Senator Nunn touched upon it. Not only is it a great personal horror they will experience, but they will have by this act reduced the chances of 240 or 250 million people to continue to remain free and alive and that needs to be stressed as well. Thank you very much.

Mr. BOYCE. Thank you.

Senator NUNN. We appreciate you being here, Mr. Dougherty. We appreciate you being here. We will wait just a minute and continue our hearing with our next witnesses.

[At this point in the hearing, Senator Cohen withdrew from the hearing room.]

Senator NUNN [presiding]. Our next panel, if they would come forward, will be Mr. Paul W. Schwegler, vice president and general manager, administrative services division, and Regis Carr, director of security, health and safety, TRW, Inc., electronics and defense sector, Redondo Beach, CA; Richard M. Welby, assistant director of corporate security, Hughes Aircraft Co.; and Gen. John W. Pauly, Air force, retired, Systems Control Technology, Inc., from Palo Alto, CA.

Gentlemen, we swear all the witnesses before this subcommittee, and if you will all stand and raise your right hand. Do you swear the testimony you give before this subcommittee will be the truth, the whole truth, and nothing but the truth, so help you God?

General PAULY. I do.

Mr. SCHWEGLER. I do.

Mr. WELBY. I do.

Senator NUNN. We appreciate, first of all, you being here. We appreciate your cooperation. We know some of the subjects this morning are not entirely comfortable, but we believe they are necessary in order to learn what you have learned in terms of these security cases. Hopefully, what you have learned will be instructive to other companies. We have thousands of companies engaged in the defense business throughout the country. We very much appreciate you being here, and we would welcome your statements.

If you would like to summarize, your entire statement will be put in the record. Mr. Pauly, if we could begin with you.

TESTIMONY OF GEN. JOHN W. PAULY, USAF (RETIRED), SYSTEMS CONTROL TECHNOLOGY, INC., PALO ALTO, CA; PAUL W. SCHWEGLER, VICE PRESIDENT AND GENERAL MANAGER, ADMINISTRATIVE SERVICES DIVISION, TRW, INC., ELECTRONICS AND DEFENSE SECTOR, REDONDO BEACH, CA; AND RICHARD M. WELBY, ASSISTANT DIRECTOR OF CORPORATE SECURITY, HUGHES AIRCRAFT CO., EL SEGUNDO, CA

General PAULY. My name is John W. Pauly. I am chief executive officer of Systems Control Technology of Palo Alto, CA. I have served in that capacity since June of 1982.

It's a pleasure to have the opportunity to testify on this extremely important matter, which is so vital, as we all know, to our national security.

I have provided a statement for insertion into the record, and with your permission, I will summarize the main points of that statement.

Senator NUNN. Without objection, your entire statement will be placed in the record.

General PAULY. Thank you, sir. by way of background, my prior experience has centered around a 35-year career in the U.S. Air Force, from which I retired in the rank of general in 1980. At the time of my retirement, I was serving as Commander in Chief of U.S. Air Forces in Europe, as well as in the NATO structure as Commander of Allied Air Forces in Central Europe. Immediately prior to that, I held several operational and planning positions within the JCS organization and in the Air Force. For virtually all of my military career, I was required to deal with classified matters on a daily basis and to use and protect documents at all levels of classification.

Systems Control Technology was incorporated in July 1981. It had been split from a larger company, Systems Control, Inc., to centralize all Government work within a totally separate management structure.

At that time, of course, the entire classified account was passed over to SCT in its own facilities, physically separated from the original company under the close supervision of the Defense Investigative Service.

Systems Control Technology is a small business with approximately 175 employees. We occupy portions of two adjacent buildings in the Stanford Industrial Park in Palo Alto. We currently hold less than 100 contracts, small and medium in size, with approximately one-third requiring access to classified material. With these dimensions, I may be able to presume to represent the small business dimension of the industrial security problem this morning.

The facts of the Harper case are well known, and I won't repeat them. However, I do want to make the point that the main function of Systems Control Technology, as a company, in this case was in actively supporting the Federal Bureau of Investigation during their investigation. The espionage had been committed several years before we came into existence. In this regard, I would also like to clarify the fact for the record that Harper and Schuler were not employees of SCT, contrary to what was stated earlier this morning.

After a case such as this, it is imperative that all possible steps be taken to identify what lesson can be learned from the experience. To do this, it is necessary, of course, to seek out the root causes or weaknesses in the Security Program which permitted this breach to happen.

Now, I cannot testify personally as to the conditions which existed in Systems Control since I had no contact with that company. Nor have I ever met or seen Schuler or Harper.

I can, however, make some observation that I believe is pertinent. Most importantly, however, it must be noted that Systems Control was provided a facility clearance by the Department of Defense in 1968, having fully met the criteria for the granting of such a clearance. That meant that the facility met certain required standards, that necessary security policies and procedures were in force, that employees had been educated in security requirements and that classified information could be properly protected.

Through the years, Systems Control was subject to regular inspections by the Defense Investigative Service and its predecessors that held that responsibility. That they were permitted to retain their facility clearance, in my mind, testifies to the fact that they were found to have had an effective security system throughout the period. Conversations that I have had with several individuals who were employees of that company in the late 1970's tend to verify that the Security Program was not only effective, but respected.

Unfortunately, all Security Programs designed to protect classified national defense information are heavily dependent upon the integrity of those individuals who the Government clears for access to the classified information.

In this case, Schuler had been cleared for access up to the secret level. She betrayed that trust without detection and, therefore, the entire security system broke down. Once a properly cleared person decides to turn against his or her country, it is extremely difficult, if not impossible, to prevent compromise of defense information.

This introduces another dimension, which is prominent in this case. It is the absolute necessity for all personnel to be constantly alert to any manifestations in their coworkers' actions which could hint that they could be a security risk. In this case, Schuler was known to be a heavy drinker and some have classified her as an alcoholic.

If I were to identify a major lesson learned in the Harper case, it would be this latter point.

Despite certain recent compromises, such as that seen in the Harper case, I believe the Defense Industrial Security Program is effective——

Senator NUNN [interposing]. Let me make sure I got that point. You are speaking to the alcohol problem?

General PAULY. I am speaking of the necessity, Senator, for individuals who come in contact with other individuals who uncover adverse information on these people who hold security clearances, their responsibility is to be alert to such information and to report it.

Senator NUNN. Well, on that point, do you believe it would be of some value—Mr. Boyce suggested here a while ago if there had been some kind of hotline for reports directly to the Government rather the company itself, if that was a well-known fact, that would be a deterrent. Do you have any kind of hotline, one directed to the Government or one directed to security personnel in the company? What is your reaction to that?

General PAULY. My reaction is based on a strong feeling on my part that management of companies, particularly small companies, where it is almost a family operation, 170 people, I know virtually all of my people reasonably well. In our case, I don't favorably support that recommendation. I feel that it could be subject to tremendous abuse. I can see hotlines reporting on establishments, for instance, a hotline for Government abuse and other misdeeds. These things are not personal. You can examine and investigate the charge of what you receive on the hotline and find it is true or false. But in the nebulous area that talks about people's personal actions and their conduct, et cetera, that is a very personal thing, and there is no way to prove or disprove it, it seems to me. I think it would be subject to abuse.

Senator NUNN. How should it work then? Why was her alcoholism not noted in a small company?

General PAULY. In my judgment, it should have been, if it was bad enough. I talked to people about the degree of her use of alcohol. Some would say she was a drinker, and others say she was an alcoholic. It should have been reported and reported up channel to the executives who ran the company and also, of course, the regulations require once it is formally registered, that it be reported immediately to the Defense Investigative Service.

I'm a believer in the structure, whereas Mr. Boyce seemed to think he supported a hotline because he felt the structure broke down. I don't agree with that part of it. I believe the people who are responsible for the management of a company who has a security clearance are the ones that are determined to be responsible, and they should be made aware. Reports shouldn't go around it in a hotline fashion.

Senator NUNN. I think he was speaking from a deterrent point of view. He was speaking as one who committed espionage and said he believed he would have been partially deterred had he believed there was a reporting system where companies could report activities that they observe.

And you are saying in your company you don't think that is necessary.

General PAULY. I think what we have done actively is to educate people that adverse information reporting is a responsibility of theirs. In a company of my size, what I would prefer is for the leadership, the management of the company not be bypassed, for them to be informed and, at the same time, the Defense Investigative Service.

Senator NUNN. How about a hotline to somebody in the top level of the company rather than the Government?

General PAULY. I would support that.

Senator NUNN. Do you have such now?

General PAULY. No, we don't, except we have the enforced open-door policy that encourages people to do it. We don't have something that you would call a "hotline."

Senator NUNN. Go ahead. I will ask questions later on this, so we don't disrupt the order on here.

General PAULY. I was to comment very briefly about my view of the Defense Industrial Security Program. I believe that despite certain recent compromises, such as the Harper case, I believe the Defense Industrial Security Program is effective within the resources that have been allocated to it. It provides a broad and solid structure for the accomplishment of the monumental tasks that has been assigned to this organization.

I believe that its inspection system provides an excellent mechanism for the Defense Investigative Service to properly oversee the program and to ensure defense contractors maintain the required degree of security.

I must add that I find the DIS structure in the field to be extremely helpful in the advisory role as well. There is no question the overall program can be strengthened with the commitment of additional resources. Certainly, such things as more frequent contact with defense companies and more frequent updates of security clearances would go a long way to improve the situation.

The first crying need, however, is to tackle the human reliability aspects. The integrity of the people cleared is intended to be the keystone of the entire security program. Instead, it appears that it is the Achilles heel in certain cases. This fact certainly indicates that priority attention should be applied here. It would follow that such things as updating security clearances and controlling the number of people who hold active clearances and have a need to know would go a long way toward improving the situation.

Since our incorporation in 1981, the SCT Internal Security Program has been maintained under the "Industrial Security Manual." We conform to the policies and procedures outlined in that document and fulfill any specific requirements which the manual levies on us.

Our managers and employees take security seriously. Security awareness is relatively easy to recognize, as I mentioned earlier, in a small company with some 175 people in which you interface with a significant percentage of those people on a daily basis.

I will cut out a little of what I intended to say on our security program to come to my final comments, which would be addressed to the efforts of the Defense Industrial Security Review Committee. Let me report that I have reviewed the recommendations of the Defense Industrial Security Review Committee and enthusiastically agree with a great majority of them. I particularly support the following:

The need to repeat and update security checks for secret clearances; the need to place more emphasis on the human reliability dimension of the problem; the need to revise the format of the "Industrial Security Manual" to eliminate much of its detail; the need for cleared employees to report all foreign travel.

[At this point in the hearing, Senator Gore entered the hearing room.]

General PAULY [continuing]. The need to expand the DOD security inspection rating system award of one of four ratings—superior, satisfactory, marginal, or unsatisfactory; and finally, the need for DIS to provide a more formal certification training program for contractor industrial security personnel.

This is particularly important in small companies where you don't have a stable of security people but only a handful. So their capability is one of great importance.

I have one to add, and it has to do with picking up some of the features of the Department of Defense Personnel Reliability Program, which was an outgrowth of the Air Force Human Reliability Program, now adopted by the Department of Defense. This provides a formalized structure for keeping a deep assurance as to the human reliability of the people that are cleared, and it has features that I think are usable in addressing the problem which this subcommittee is addressing.

The recommendations with which I do not concur have to do with the proposal to create separate advisory roles for DIS representatives as opposed to the inspector role and the proposal to establish a national industrial security hotline program.

The committee appears to have examined every possible aspect of the problem, and I believe by and large, their recommendations will have a positive impact on the serious efforts to improve industrial security.

In addition to that, Senator, I would like to ask permission to either submit for the record or have the opportunity to discuss several earlier questions and answers having to do with systems control technology that I think were somewhat misleading. I would like to have that opportunity on one form or the other.

Senator NUNN. We would be delighted to have that for the record. If you would like to say something later this morning, we would like to have that.

We had originally scheduled as a witness for today General Stilwell, a man with vast experience in combat and combat command in the Department of Defense, formerly Deputy Under Secretary of Defense to be accompanied by Britt Snider, Director, Counterintelligence and Security Policy, Department of Defense. I believe this panel is going to consume most of the time the Senators have left today. Because of his expertise, I want to have plenty of time to ask General Stilwell questions on these issues. I will be available to remain today to do so, if General Stilwell is going to be inconvenienced by a postponement. However, I would hope that we can reschedule, General Stilwell, at a date that is convenient for you because we are going to be trying to get some policy recommendations here that are most important.

It would be very helpful to us to not only hear your views but be able to take what we have gathered in this hearing in terms of suggestions and ask your opinion on those.

So if it is not too inconvenient to you, I would ask we defer your appearance until a date that is convenient for you, hopefully in the next 2 or 3 weeks.

General STILWELL. Fine.

Senator NUNN. Thank you very much.

Our next witness is Mr. Schwegler of TRW. Mr. Schwegler, we will be delighted to have your statement. I will be coming back to ask questions.

Mr. SCHWEGLER. Mr. Chairman, members of the subcommittee, I am Paul W. Schwegler, vice president and general manager of the administrative services division, electronics and defense sector of TRW in Redondo Beach, CA.

For our defense business, I am responsible for 27 locations and more than 25,000 employees. I am pleased to be here today to testify on behalf of TRW in response to the subcommittee's request. With your permission, I would like to submit my written statement for the record and briefly summarize key points and several recommendations made in my written testimony.

Senator NUNN. Without objection, your entire statement will be included as part of the record.

Mr. SCHWEGLER. Thank you, Senator. I will focus on TRW's procedures for special security programs, some key aspects of the Boyce case and comment on some recommendations of the Department of Defense Industrial Security Review Committee.

First, let me summarize TRW's security procedures for special security programs. When a company like TRW is requested by the Department of Defense or the intelligence community to bid on a special security program, we receive the request via a courier. If we decide to bid, all personnel selected to work on the project are submitted for clearance by the Government for the security access level appropriate to the program.

[At this point in the hearing, Senator Nunn withdrew from the hearing room. Letter of authority follows:]

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, DC.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive session hearings without a quorum of two Members for the administration of oaths and taking testimony in connection with hearings on "U.S. Government Personnel Security Program." These hearings are to be held on April 16, 17 and 18, 1985.

BILL ROTH,
Chairman.
SAM NUNN,
Ranking Minority Member.

Mr. SCHWEGLER. The responsibility to clear and approve personnel for a special security program rests with the appropriate Government agency involved. Once an employee has been cleared, the employee is briefed indepth by approved security personnel on his or her security obligations.

We consider TRW security practices relating to personnel, documents, and physical security to be rigorous and exact. In addition to the briefings for special security programs, we outline espionage and related statutes to new TRW employees as a part of their initial orientation and provide each employee with a copy of a TRW booklet containing excerpts from the U.S. espionage statutes.

In addition to the personnel clearances and briefing process, we have stringent document security and physical security procedures complying with the Government's requirements with special compartmentalized facilities, and the Defense Investigative Service Program, which covers building structure, access, and communications security.

In both cases, our security requirements program rigorously complies with all of the Government's requirements.

Important as all these security procedures are, they cannot ultimately assure the protection of the Nation's classified assets. Sound security procedures are certainly essential, but in the final analysis, it is the individual's personal integrity and loyalty to our country that provides this guarantee.

[At this point in the hearing, Senator Nunn entered the hearing room.]

Mr. SCHWEGLER. That's why we put enormous emphasis on security awareness and motivation programs for our employees. I'm proud to say that since TRW's inception, more than 75,000 employees have gone through the kinds of procedures I just described. Only one, Christopher John Boyce, has, to our knowledge or that of the Government's, ever committed treason against his country. We are glad to outline some of the lessons learned from the Boyce incident, but we would emphasize to you that the case is now more than 8 years old and the intervening years have brought improvements in Government and private-sector security practices and procedures as well as improvements afforded by technology.

Senator NUNN. Let me ask, if I could, just interrupting right there, I understand improvements have been made, and those improvements are most welcome, but when you say in your statement: "despite our view that our security procedures were sound prior to the Boyce case," that gives me pause. That bothers me because if you feel they were sound prior to the Boyce case, after all we heard this morning, that makes me wonder how serious you have been about correcting those things, because that which is sound prior to security breach doesn't need correcting.

Mr. SCHWEGLER. Senator, as a result of the Boyce incident and shortly thereafter, the U.S. Government sent in an investigation team, which I am advised that the investigation performed was one of the most stringent investigations that had ever been done in the private sector.

The conclusions reached as a result of those investigations suggests strongly that many of the things which Mr. Boyce dealt with this morning were exaggerations, and I think if you had the opportunity to review the testimony of the trial of which Mr. Boyce was a part of, you would see that there are similarities between what was said there and what was said here this morning.

Additionally, I would remind all of us of Judge Keller's comments at the end of the trial regarding the court's views of the veracity of Mr. Boyce.

Senator NUNN. Didn't the investigation by the Government after the Boyce case reveal that you had severe drinking problems in the vault?

Mr. SCHWEGLER. The investigation by the U.S. Government, Senator, after the Boyce case, did not reveal that we had severe drinking problems in the vault.

Senator NUNN. How did they characterize the drinking problems?

Mr. SCHWEGLER. A limited use of alcohol on the premises.

Senator NUNN. Limited use of alcohol——

Mr. SCHWEGLER [interposing]. Let me elaborate further. There were two bottles, empty bottles, liquor bottles that were found in the vault after the Boyce case. Whether there was alcohol in them and consumed in the vault, I can't testify to that. Additionally, through the Government's investigation, as well as our own self-analysis, we uncovered two additional situations where liquor had been on the premises, but no more than those two.

Senator NUNN. Did the Government investigation after the Boyce case find there had been poor security supervision?

Mr. SCHWEGLER. Senator, that's correct. Poor security supervision in terms of Mr. Boyce's immediate supervisor who, as Mr. Boyce mentioned this morning, resigned from TRW. I believe Mr. Boyce said he was transferred, which implies TRW transferred him. That's not true. He resigned from TRW prior to Mr. Boyce's arrest.

Senator NUNN. It seems to me when they find drinking and when they find poor supervision, that is more than just a simple, technical problem. What about badge control? My understanding is that the Government investigation found very poor badge control.

Mr SCHWEGLER. As was mentioned in our written testimony, the Government did find, Senator, that we needed to sequentially prenumber the blank badge stock so that there would be stronger controls on that stock, and that was done immediately.

Senator NUNN. But you stand by your statement that: "Our security procedures were sound prior to the Boyce case"?

Mr. SCHWEGLER. We believe that to be true, sir.

Senator NUNN. Does that mean when a 21-year-old young man is hired by one of our defense contractors, that we have no way to protect against massive amounts of documents being taken out of vaults; that we have no way to protect against photographs of those documents; that we have no way to protect our Government, and our country, and our people against those kinds of security breaches? That is the conclusion one has to reach if you really mean this, if you had sound security practices.

Mr. SCHWEGLER. Senator, again, the Government investigation found a limited number of variances to their requirements.

Senator NUNN. Like poor supervision.

Mr. SCHWEGLER. That was one of the observations that was made by the Government inspection.

Senator CHILES. Were their requirements worth a hoot then?

Mr. SCHWEGLER. Senator, subsequent to the Boyce incident, a number of changes had been made; changes which, in our view, are positive changes. Albeit, the Boyce situation is a national tragedy; I think even more tragic than that would be if we didn't take advantage of the lessons learned, and in many of these, recommendations that have subsequently been included in the industrial security program are enumerated in our written testimony.

Senator NUNN. But you truly believe your procedures were sound prior to the Boyce case.

Mr. SCHWEGLER. Senator, I do.

Senator NUNN. And you were responsible for this; were you there at the time? Are you reporting after the fact, or are you reporting based on personal knowledge?

Mr. SCHWEGLER. I was not there at the time that Boyce was arrested, Senator. I did arrive in California very shortly thereafter in, I believe, the September timeframe and, furthermore, I am very familiar with the results of the investigation.

Senator NUNN. Did you supervise the internal investigation, or did you have an internal investigation?

Mr. SCHWEGLER. We did have an internal self-analysis, Senator. I did not supervise that.

Senator NUNN. Would you furnish that to us for the record?

Mr. SCHWEGLER. Yes, Senator, we would be pleased to do that.

Senator GORE. Would the Senator yield on this line of questioning?

Senator NUNN. Yes.

Senator GORE. Did you hear Mr. Boyce's statement that one of his fellow employees put a photograph of a monkey on his ID card and used that to get routinely in and out of the facility?

Mr. SCHWEGLER. Yes, I heard that, Senator.

Senator GORE. And that other cards were fabricated, and that on one occasion, when soneone who was not cleared came and asked for security cards without any sort of clearance documentation, he was disciplined for refusing to give a clearance card in the absence of the adequate documentation?

Mr. SCHWEGLER. Yes; I heard him say that, Senator.

Senator GORE. And those procedures are still all right, in your mind?

Mr. SCHWEGLER. Senator, one, with regard to the badge which Mr. Boyce referenced. I have seen that badge, and I find it extremely difficult to believe that you could gain entrance to our facility by using that badge.

Senator GORE. But his testimony was that it was used to gain entrance, and the procedures were "just a joke," to use his words.

Mr. SCHWEGLER. Senator, again, I reference the Government investigation as well as our own self-analysis and that was not found to be the case, sir.

Senator GORE. You used the phrase "limited variances." That sounds like a bureaucrateze for violations. Is there a difference between limited variances and violation of security procedures?

Mr. SCHWEGLER. Yes, there is, Senator.

Senator GORE. So your view is that everything was fine then but it is even better now?

Mr. SCHWEGLER. Senator, as I mentioned before in our written statement, we very clearly display the kinds of variances that the Government found as a result of their investigation.

Additionally, we talked in specifics about the recommendations which we made to the Government regarding improving practices and those recommendations are in place right now and operable.

Senator GORE. You used the word "limited" in response to Senator Nunn's question about the drinking in the vault as well. You said there was just limited drinking. Was there limited use of the shredding machine to make mai-tais and other cocktails or extensive use?

Mr. SCHWEGLER. Senator, again, the Government investigation did not uncover that that machine was used to mix alcoholic beverages in.

Senator GORE. Did you see the wine stains on the wall?

Mr. SCHWEGLER. Senator, I have no evidence that those stains were a result of wine.

Senator GORE. It doesn't look like limited wine—[laughter]—in the photograph? It looks like it corroborates his testimony that it was a kind of a wild scene in there and that security procedures really were "a joke." I believe I understand why you are saying, it would certainly be refreshing to have you say:

> Yeah, we really messed up; things got very lax here and we learned a lesson from this case. We can't ever be expected to be held responsible for the actions of a determined traitor, but we can be held responsible for lax security procedures that would put second thoughts in the minds of people who might consider treasonous actions, and we didn't do a very good job here. We have tried to straighten it up in response to this tragedy.

Instead, you take the approach that we didn't really make any mistakes at all; everything was great and now it's even better. I think I understand why you are saying that. We are trying to conduct a very constructive investigation here, and I think so far it has been. I think that will be evident in the recommendations that come out of this subcommittee. However, we could get a little more help from the contractors if you all were a little more candid, I would say, with all due respect.

I appreciate the time.

Senator NUNN. Just one other question, and then we will go on because I am interested in the steps you have taken to correct these "limited number of variances."

The 21-year-old, do you have any procedure about having people with that age with no prior job experience involved in top secret specialized-type information now? Has any change come out of that?

Mr. SCHWEGLER. Senator, yes, there has been a change. One, which as a matter of practice we levied on ourselves. Given the kind of sensitive position that Mr. Boyce was in, we have quickly concluded that, albeit the age question has not statistically been demonstrated that folks that age are more untrustworthy than others, we now will not put a person in that kind of a role until we've had some place of 12 and 18 months to evaluate that person's stability.

Senator NUNN. You think experience is the key, not the age?

Mr. SCHWEGLER. I think experience is clearly, Senator, one of the things that can be measured, if you will, in a background investigation.

Senator NUNN. Why don't you go ahead.

Senator CHILES. I just wonder on that same line, can you tell me who was disciplined and whether anybody was fired as a result of the Boyce case?

Mr. SCHWEGLER. Yes, Senator. As I mentioned, Mr. Boyce's immediate supervisor resigned from the company prior to Mr. Boyce's arrest. So there was no opportunity to take disciplinary action there, if it would have been warranted.

Second, again, as a result of our own self-analysis as well as the Government's investigation, it became clear that the weak link in the management chain was clearly Mr. Boyce's immediate supervisor and that there wasn't evidence or sufficient evidence beyond that which would warrant taking disciplinary action.

Senator NUNN. So other than Mr. Boyce's immediate supervisor who resigned prior to his arrest, no one else was disciplined and there——

Mr. SCHWEGLER [interposing]. There were two other persons, one of whom worked in the communications center with Mr. Boyce that resigned after Mr. Boyce's arrest, and the second person was an office support person who also resigned after Mr. Boyce's arrest.

Senator NUNN. Why don't you go ahead.

Mr. SCHWEGLER. In addition to the Government's investigation, TRW also conducted a self-analysis to determine what improvements could be made. What we learned and recommended as a result are outlined in detail in our written statement.

The resulting system includes not only changes recommended by the Government, but also changes we made on our own and recommendations we made to the Government for changes in overall industrial security practice to improve the effectiveness of the National Security Program.

We believe that the changes that have been made to industrial security practices significantly improve the protection of highly sensitive Government information in special Security Program areas, but the Boyce case has also reaffirmed to us the important element of personal integrity in an effective security program, and we and other defense contractors work closely to develop awareness programs that will address this essential component of our national security system.

Last, we would like to comment briefly on a report of the Department of Defense Industrial Security Review Committee. Many of the recommendations address internal Government procedures on which we have no comment. However, we do offer the following for your consideration:

One, we would recommend expansion of the existing investigative criteria presently used to grant secret clearances and we believe the national agency check should be augmented in some manner. For example, a recent change in top secret clearance procedures requires an interview with the candidate. This might also be considered for granting a secret clearance. We would, however, be concerned by any change that would significantly lengthen the clearance process because any additional delays slows program performance and increases costs to the Government. Two——

Senator NUNN [interposing]. We have a strong interest in that and a number of people being cleared, time, so forth, productivity loss by delay in clearances. Do you have any records to indicate the time lag in your clearance procedures and how that relates to productivity or cost?

Mr. SCHWEGLER. Senator, if we do, I will be more than pleased to submit those to you.

Senator NUNN. If you could. Any of those who have that, it would be helpful in terms of giving us your experience, the time required for clearances and costs associated with that.

Mr. SCHWEGLER. Two, although the need-to-know principle is effectively applied in special security programs, it should be more strictly enforced in dealing with all other types of classified information, both in industry and Government.

Information should be provided only to personnel who have an absolute need for it.

Three, a uniformed security motivation and awareness education standard should be established for industry and Government. Greater emphasis should be given to the security clearance—excuse me, given to the security awareness and motivation of all personnel possessing a clearance and having access to classified information.

TRW has developed such a program which ranges from briefings conducted by the FBI on threats to our society to the use of a wide range of internal communication tools.

Four, a standard set of minimum security regulations in non-SCI areas applicable to Government contracting in all Federal agencies could be developed covering the entire spectrum of Government-imposed security requirements and guidelines.

Five, a Government-wide adjudication standard that is well understood by both the public and private sectors is needed. The adjudication process should be strengthened to include more effective means for removal or denial of clearances.

As we know from past history, no security system is invulnerable. Both the private as well as the public sector must never become complacent.

[At this point in the hearing, Senator Chiles withdrew from the hearing room.]

Mr. SCHWEGLER. It is my view that the implementation of these recommendations would further strengthen our national security.

Mr. Chairman, thank you very much for the opportunity to appear before your subcommittee. I would be happy to answer any further questions you may have.

Senator NUNN. Thank you very much. Mr. Welby?

Mr. WELBY. Mr. Chairman and members of the permanent subcommittee, my name is Richard Welby, assistant director, corporate security, Hughes Aircraft Co., El Segundo, CA. I am a former special agent of the FBI. I am here at the invitation of this subcommittee to testify on behalf of Hughes Aircraft Co. I would like to give you a brief description of the Hughes Aircraft Security Program, and to keep it brief, I would like to submit my opening statement, plus six volumes I was asked to bring with me.

Senator **Nunn**. That will be included in the record, without objection.

[The volumes referred to were marked "Exhibit No. 26" and may be found in the subcommittee files.]

Mr. **Welby**. Hughes Aircraft Co. has capabilities in advanced electronics, space and communications, missiles and avionics, air defense, command and control, industrial electronics, and basic research. Its activities span more than 1,500 projects and include over 12,000 separate products, services, and functions.

Hughes employs approximately 74,000 employees, including over 23,000 on the scientific and engineering technical staff who work in fully equipped facilities encompassing more than 19 million square feet of floor space. The company is made up of 7 major product organizations.

There are 60 cleared company facilities with established Security Practices and procedures outlining the requirement of the Defense Industrial Security Program. Approximately 1,035 security personnel are directly assigned to administer and implement the company security program for meeting the requirements of the Defense Industrial Security Program.

Exhibit 1 will set forth the personnel, physical, and information——

Senator **Nunn** [interposing]. Without objection, it will be numbered appropriately.

Mr. **Welby**. Company facilities are cleared by the Government at the top secret and secret level with equivalent storage capabilities which qualify the company to bid, receive, and perform on contracts requiring access to classified material at these levels.

The Defense Investigative Service cognizant security offices inspect all areas of the company's implementation of the Defense Industrial Security Program on a biannual basis. Periodical inspections are also conducted on the company's Arms, Ammunition, and Explosives Program, Industrial Facilities Protection Program, and Operations Security Program, which is known as OPSEC.

The company conducts biannual self-inspection of the Government security program and also an annual inventory of all top secret and secret material.

In addition, employees are issued statements of their secret document holdings every 3 months. Currently, 2,300 employees have secret documents in their custody.

The company is currently performing on approximately 1,200 prime contracts and subcontracts with U.S. Government user agencies and other major contractors which require access to classified information.

The company issues over 1,400 purchase orders to subcontractors each year involving procurement of classified parts and services in support of prime and subcontracts.

In support of these contracts, company security organizations process approximately 10,000 incoming visits and 18,000 outgoing visits annually.

Company security organizations are responsible for conducting investigations of administrative security infractions, violations, thefts, sabotage, and violations of company rules. I would like to introduce a summary of the Bell case as one of the exhibits.

Senator **Nunn**. Without objection, it will be part of the record.

[The information referred to follows Mr. Welby's prepared statement.]

Mr. **Welby**. The Hughes investigation of the Bell case indicated the incident did not result from a weakness in our security program or classified document accountability system, but from the willful security violations by a long-time employee.

Our investigations revealed that William Bell intentionally violated company and Government security regulations by illegally removing classified documents from company premises. There is just no way to prevent such unauthorized removals short of conducting a physical search of each employee as he or she departs company premises.

Our investigations of the incident revealed the secret documents charged to Bell were properly accounted for and surrendered by him at the time of his termination.

We believe our security and classified document accountability systems function efficiently and effectively. However, we feel the best system still depends upon the integrity of the employee beginning from the time he was screened, hired, investigated, security indoctrinated, and granted a secret and top secret clearance.

I have two other documents I would like to introduce at the conclusion.

Senator **Nunn**. They will be accepted for the record.

[The documents referred to follow Mr. Welby's prepared statement.]

Senator **Nunn**. Let me address a few questions to you gentlemen. We appreciate all of you being here today, as I mentioned. I have other questions for the record. But I do have some I would like to ask.

Paragraph 6(b)(1) of the "Industrial Security Manual" requires that contractors report adverse information or derogatories on their cleared employees to the Defense Industrial Security Agency. DIS has voiced concern over the great lax of 6(b)(1) reports by contractors.

Starting, General Pauly, with you, what is your practice in terms of making those kinds of reports as required by DIS?

General **Pauly**. Basically, we acknowledge that responsibility and my insistence is that I be informed at the same time. That is a responsibility of our security people. I think as that particular directive reads that the security individual will advise DIS, and my insistence is I be advised at the same time.

I have a reason for that. Not that I can override the report to DIS, nor would I ever have an intention to do that unless it appeared to me to be a gross example of personality conflict or something that didn't meet the eye. I want to be informed so that at that point, I can put on a rider or some sort of qualification or explanation to DIS as I see it as the executive officer and at the same time the report goes in.

Senator **Nunn**. Mr. Schwegler?

Mr. **Schwegler**. Senator, we also acknowledge that requirement, and I'm pleased to say perhaps 3 weeks ago, perhaps at most, I was just debriefed on one of the 6-month DIS inspections in our Redondo Beach facility, and the team leader made a very explicit point to acknowledge that TRW is one of the more aggressive contractors in reporting under that provision.

Senator NUNN. So your company is complying and doing so, you think, in adequate fashion?

Mr. SCHWEGLER. Mr. Chairman, yes, sir.

Senator NUNN. Mr. Welby?

Mr. WELBY. Senator, I believe we have a very active Security Program at Hughes. It starts at the very top of management, the chairman of the board right down to the lowest level employee. I think we really are in step with the program. In fact prior to my testimony, I informed the staff that last year, we reported 120 violations to the Government under paragraph 6(b)(1).

Senator NUNN. 120?

Mr. WELBY. Yes, sir.

Senator NUNN. Could each of you furnish for the record your own record last year?

Mr. SCHWEGLER. Mr. Chairman, we will.

General PAULY. Yes.

Senator NUNN. Mr. Welby, in the case of Hughes, William Bell told us that he had, according to him, "all the signals, all the classical reasons" for being a spy, including financial difficulties, followed by unexplained affluence, job dissatisfaction, friendship with a Polish national. All of these things were present in the Bell case, obviously after the fact.

Did Hughes ever know of any of these or ever make any report on this to the DIS?

Mr. WELBY. Senator, the security department at no time was furnished information such as contained in the allegations and statements made by Mr. Bell concerning his affluency, association, et cetera. We had no knowledge.

Senator NUNN. There was no knowledge of that at any time?

Mr. WELBY. No, sir.

Senator NUNN. So there was no report on it?

Mr. WELBY. No.

Senator NUNN. Bell had a certain friendship with a Polish national, Mr. Zacharski. Obviously, the Government was aware of the fact that this Polish national was an intelligence officer and they also knew Polamco was a suspect firm.

Was Hughes ever notified of this by the Government?

Mr. WELBY. No, sir.

Senator NUNN. Do you receive intelligence briefings on suspected individuals in the company by the Government? Have you ever had that experience?

Mr. WELBY. If I can rephrase that, DIS makes available to industry an unclassified document which lists the names of foreign national companies doing business in the United States. The most recent one was a few weeks back. I don't recall the exact date. It has not been a continuous thing going back to the Bell case.

Senator NUNN. So Hughes gets no regular briefing on classified-type suspicions from the Government?

Mr. WELBY. No, sir.

Senator NUNN. How about TRW, do you get any?

Mr. SCHWEGLER. Mr. Chairman, we do, but I would quickly add that I think that is an area clearly that could be improved upon. If the private sector does not take the initiative to go seek out these briefings, particularly small corporations, I think would be remiss. We do take the initiative, and I think it is an important part of our awareness program.

Senator NUNN. You ask for those briefings?

Mr. SCHWEGLER. That's correct, Senator. And also, Mr. Chairman, we are approached by various Government agencies who participate in our awareness programs and offer those kinds of briefings.

Senator NUNN. Those briefings take place here in Washington? Do you come here for them or are they done on location at your company?

Mr. SCHWEGLER. Mr. Chairman, they are done at the location of the company.

Senator NUNN. By different security agencies or primarily DIS?

Mr. SCHWEGLER. Mr. Chairman, ranging from the Federal Bureau of Investigation to the National Security Agency.

Senator NUNN. Do you have them set up on a routine basis or by request?

Mr. SCHWEGLER. They are programmed, Mr. Chairman, into our awareness and motivation programs.

Senator NUNN. So they are done on a regular basis?

Mr. SCHWEGLER. That's correct, Mr. Chairman.

Senator NUNN. And the Government does cooperate?

Mr. SCHWEGLER. The Goverment does cooperate, Mr. Chairman.

Senator NUNN. Hughes doesn't have anything like that?

Mr. WELBY. Senator, your question, I believe, does the Government provide such briefing. Because of what they don't tell us, we contact them. We've had many, many briefings by the Government after the Bell case. We then looked at our whole program to find out where did we go wrong.

Senator NUNN. Are those briefings on classified matters, suspicions, so forth?

Mr. WELBY. Yes, Senator.

Senator NUNN. So you have a similar program?

Mr. WELBY. In fact, with another contractor we shared one whole day with Government on the same issue.

Senator NUNN. General Pauly?

General PAULY. Yes, sir; we have briefings which are provided by DIS regularly, scheduled roughly every 6 months or so. We did talk to our poeple several times during the Harper investigation and got some unofficial inputs from the FBI. We request them; and DIS schedules them. I might add, that our most recent one I thought was superb and had none of the faults which Mr. Boyce seemed to want to belabor. It was a business-like, factual, professional job. It had to do——

Senator NUNN [interposing]. Was that a briefing of your employees or management?

General PAULY. A briefing of all of my people, sir. Names were taken and a roster kept. The absolute maximum number of people not away on trips somewhere did receive it. It was well received. It stimulated a great deal, I think, of additional awareness by the employees at all levels. In fact, I was surprised it went over so well and stimulated—the reaction was tremendous, in my view.

Senator **Nunn**. General Pauly, you acknowledged in your statement that Ruby Schuler was a known alcoholic to the extent she drank on the job. Was this ever reported under 6(b)(1)?

General **Pauly**. No, Senator, it was not, to my knowledge. Again, this was before my company was created. It was a different location, a different company, and the only thing I can go on is the information which I gleaned from the FBI investigation indirectly.

My understanding is that it was not reported. I have asked people who have known her and the usual answer you get, yes, we know she did drink. How do you draw the line of how much is too much? They did not feel it was of sufficient importance or danger to have made it a matter of record under that provision.

Senator **Nunn**. You weren't there at the time?

General **Pauly**. I was not, sir.

Senator **Nunn**. Was there anything on any of your company forms that indicated anything about her wealth, her expensive jewelry, bundles of bills in a safe deposit box, trips to Mexico with Harper on Lear jets? All of that, did you have any reference to that in the files anywhere? Did the company ever know about that?

General **Pauly**. The files we inherited when SCT was created, which went with the classified account, did have a register of her trips abroad. To my knowledge, that was the only information—there was no indication in that file of her wealth and what have you. That file, I believe, was turned over to the FBI.

Senator **Nunn**. Do any of you have any suggestions about form 6(b)(1), any ways you would change it to strengthen it, anything that is a burden to you that is unnecessary? Do you have any suggestions, or is that form and your company's compliance with it satisfactory now?

General **Pauly**. I would like to comment on that, Mr. Chairman, and it goes back to an earlier comment. It deals with the lack of appreciation of what is covered by this. No matter how often you explain to people, the definition of "adverse information" is in the eyes of the beholder.

I've talked to people, "What is your understanding?" Well, you get various answers. I'm concerned about the rights of the individual who, because of some misconception of what we are after here, is reported and it is made a matter of record.

I would like, as I stated earlier, some discretion on the part of the people in authority within the companies, particularly in my case, to evaluate it at that level before it is made a matter of record with DIS. That is the only reservation.

I understand the need for it. It is very important as has been identified, as far as the Schuler case is concerned, but on the other side of the coin, I am just very sensitive and concerned about possible abuses among the employees by reporting people unjustly or reporting them under criteria that is not fully understood to be in the spirit of the directive.

Senator **Nunn**. So now you review that before it goes, or you review it after it is already on the way?

General **Pauly**. Same time, sir. If one is reported, they come to me and I say, well OK, I want to look at this for an hour, whatever, to see if I want to put on an added note.

Senator **Nunn**. Do you have the right to add a note?

General **Pauly**. Well, sir, to my knowledge, we have not had such a report since I've been associated with this company. So I've not exercised it. Those are the directions that I put out. I believe, inherently, I have the right to add one.

Senator **Nunn**. You are saying that you would like the additional right to be able to use your discretion to eliminate that report from the security people?

General **Pauly**. Yes; that's my recommendation.

Senator **Nunn**. Mr. Schwegler, do you have a comment on that?

Mr. **Schwegler**. Yes, Mr. Chairman, I do. I would join General Pauly in most of what he said, particularly with regard to respect for the rights of privacy of the individual. However, I think it would be helpful to the private sector as well as to the public sector if 6(b)(1) was more explicit in its definition of adverse information.

I believe, again, as the General said, oftentimes what is adverse is in the eyes of the beholder. And it is not clear to me that that ought to be the case.

Senator **Nunn**. Would you agree with General Pauly's recommendation that the form be reviewed at a high level to be able to use discretion to eliminate certain information that was otherwise going to be reported?

Mr. **Schwegler**. Mr. Chairman, the form currently is reviewed at a high level in our corporation, the director of security. I am not at all certain if 6(b)(1) was more explicit that I would join my colleague in advocating the discretionary rights of the private contractor.

Senator **Nunn**. So you think if it were more explicit, that would cure the problem?

Mr. **Schwegler**. Mr. Chairman, I'm not sure it would cure the problem; I think it would bring added value to the whole process.

Senator **Nunn**. Mr. Welby?

Mr. **Welby**. We don't seem to have any difficulty with it, Senator. The responsibility lies with what is known as the facility security officer for the corporation, which I am at Hughes Aircraft. At TRW it is Regis Carr. This is not something that just came into being. It became more definitive in the last year or two in our discussions with DIS inspectors. I think it is something being addressed at the DIS level. If you're cleared, of course, we have a responsibility to report it. I don't think we have problems with what to report. I think it is pretty clear from experience what you report.

Senator **Nunn**. We had testimony yesterday in the form of a recommendation that there be some incentive on the contracts that are bid, some incentive for contractors that receive the low bid to perhaps separate out the security costs. The statement was made that there is a disincentive now for companies to engage in extensive security; that that is simply added cost and puts them in a poor competitive position in bidding on contracts.

Let me start at this end, Mr. Welby. Do you have any comment on that?

Mr. **Welby**. No, I don't, Senator.

Senator **Nunn**. Does that mean you agree with the suggestion or disagree with it? The suggestion was there is not enough incentive;

the contractors have an incentive not to take steps for security reasons, at least, to economize in every way possible and skimp on security.

Mr. WELBY. I disagree.

Senator NUNN. What are the incentives you have to maintain good security then?

Mr. WELBY. Well, I think it's a tool. But as we talked earlier, the DIS people have satisfactory versus unsatisfactory ratings. I know the corporation expects from management people, supervision in all areas, et cetera, to maintain a certain credibility. We feel the rating system certainly keeps us in that arena.

Senator NUNN. Mr. Schwegler, do you have any comments one way or the other on that suggestion?

Mr. SCHWEGLER. Mr. Chairman, yes. Currently within a significant fraction of our special compartmented special projects, we do have some clauses for security built into the contract provisions. We have found that has brought added value in terms of the management attention, if you will, that security is given. So I guess my observation would be that is something that ought to be considered in other contracting arrangements.

Senator NUNN. You think it is worthy of consideration?

Mr. SCHWEGLER. Mr. Chairman, I do.

Senator NUNN. General Pauly?

General PAULY. I agree with Mr. Howe who testified yesterday on that point that it's important that companies are not penalized for going overboard, if you will, or beyond the requirements of the criteria that is established by the Defense Department.

So I think that is an excellent suggestion, particularly in the small-business situation. Putting a guard force in, for instance, in my company would be very, very expensive. But there is a dimension I would like to introduce to this.

The Defense Department has established certain criteria that we meet and it is very difficult to take additional steps. We do some things that we are not required to do in my company, but it is very difficult, if you meet the criteria, to get too enthusiastic about outlays of great amounts of money beyond the criteria in the interest of the overall problem. I think that is very, very important that these criteria are carefully thought out and are inspected regularly. We go to the DIS for advice, all of us. I know in our case, we meet the criteria. But Mr. Howe's suggestion intrigues me because somewhere subconsciously there has to be a case there, and I think some stipulation that those charges above and beyond a certain level could be taken out of the overhead and G&A computations is a valid one.

Senator NUNN. Thank you very much. Senator Gore, let me yield to you.

Senator GORE. Thank you, Mr. Chairman. We also have heard about another kind of incentive that contractors have. That is to process their employees for clearance, clear them at the highest conceivable level.

Do you agree there is an incentive to get more employees cleared at the highest level possible?

Mr. WELBY. Senator, in our company, before it is submitted to our department, the clearance branch—there are two steps—of course, you execute the appropriate forms. Prior to doing that, direct supervision, which we call middle management or supervisors, has to request the clearance for a certain level of a certain person——

Senator **Gore** [interposing]. Finish if you want, but the question is not really about what procedures you have. Isn't there, in fact, an incentive for you to get as many——

Mr. **Welby** [interposing]. No. Supervision has to account for the level of clearance. If they say you need a secret clearance, then there has to be an appropriate contract assigned to and why so and so should have a clearance. If supervision says this person needs a top secret, but will be working only on secret material, that contract will indicate it is only at the level of secret. Even if they want to do it, they can't do it, according to our procedures in our company.

Senator **Gore**. Go ahead.

Mr. **Schwegler**. Senator, I think the basis of that question, at least as I interpret that question, is the whole notion of proliferation of clearances——

Senator **Gore** [interposing]. Right.

Mr. **Schwegler** [continuing]. And too many clearances.

Senator **Gore**. There are a million employees of private contractors now who have secret or top secret security clearances, and we have had testimony that given the fact that other contracts are going to be coming down the line and there are delays, long delays built into the clearance procedure. There is a natural incentive for contractors to have as many of their employees as possible cleared that will enable them to move right into work that comes without having to wait for the delays. Isn't that an incentive that exists?

Mr. **Schwegler**. Senator, in my view, yes, that is an incentive. Flexibility is extremely important to be able to apply your resources to a variety of programs at any given point in time. However, it would be our view that if the need-to-know principle was more effectively applied, as it is applied in the SCI environment, that might begin to deal with some of the core of this problem.

Senator **Gore**. I appreciate your candor. I think that is a helpful recommendation. Did you want to address the same question?

General **Pauly**. Yes, Senator, I would like to very much. I am glad to see this question of need to know brought out. It is not clearly understood, I don't believe, what we are saying here. In my company, if we bring a new person in and some of my divisions do nothing but classified work, others do some classified and some unclassified, so you have to make a judgment when you bring people in where you have in mind using him and also what the probability is that he be required to have a clearance.

So you end up, as time goes on, with a certain balance of people that are cleared and those that are not. Contracts come and go, but the point is that the need to know is another measure that we use. If there is a need to know, then that clearance is an active clearance in the company, and the determining person in that is the program or project director, and, as an example, I have something like a hundred and some odd people who have clearances on the books, but we only have something like 45 or so that have a need to know at this time. They are the only ones that have access to the particular safes, for instance.

So it is a discipline level which is very important to this.

Senator GORE. When you request clearance for one of your employees, the Government pays all those costs of the checks and the background checks and all of the procedures?

General PAULY. Yes; that's correct.

Senator GORE. Regardless of how many employees you send over for clearances, the Government still picks up the cost for all of them, right?

General PAULY. That's my understanding; yes.

Senator GORE. As is true with all these companies, the companies pay nothing, regardless of how many employees are sent over for clearance. There is no limit on it. Would a quota system that sets some reasonable determinative limit and then assessed the contractors for the investigative costs above that quota? That would provide some kind of counterpressure to hold down the proliferation of security clearances among private contractors.

I will interpret your silence as agreement. [Laughter.]

General PAULY. It is one that takes a little thinking through.

Senator GORE. Yes; I can imagine it does. I understand you would probably not like the idea, but it has some merit, don't you think?

General PAULY. I would say it has some merit. Of course, the end result is that it adds to the overhead rate, which the Government ends up paying.

So the expenses don't go away. If the company has a valid cost, as this would be, it would seem to me, then it would add to our overhead rate and the companies, particularly in my case, are very sensitive to that because the higher that rate goes, the more noncompetitive you become.

Senator GORE. Of course, all your competitors would face the same expense and you could be more competitive by holding down the number of employees that you submitted for clearance.

It is true that the bill would be passed on in charges, but it would be added to your overall contract cost, and I know that the size of defense contracts is not much of a disincentive, but presumably there is some limit that is reached that you would be sensitive to that.

Do the other two witnesses want to comment on this idea?

Mr. SCHWEGLER. Senator, yes, I would like to. I think certainly that's an alternative what you put forth, and it would provide a counterpressure, as you mentioned. However, it would seem to me that we ought to look at what the range of alternatives are and how the coupling of various alternatives would present a positive effect on this perceived problem.

Senator GORE. Very good.

Mr. WELBY. It sounds like the devil's advocate, Senator, in the DOD arena at Hughes. I can assure you the Government recently at an AI meeting, they kept beating on us about the number of clearances being processed for employees at all levels. We brought the message back to upper level management to limit, as I said earlier, not to repeat myself—to limit the number of clearances.

We said we would like to have them all, but we don't. We try to stay with the ground rules.

Senator **Gore**. I appreciate that response, but I am not impressed with the effectiveness of constant beating upon the contractors by DOD because that could stop next year, and wear out in its effectiveness.

The DOD report found that from 90,000 to 95,000 contractor personnel cleared for top secret did not have frequent access to top secret information, and the 35 to 40,000 of those with top secret clearances never had access to top secret information. Clearly, that is an indication the proliferation has reached the point where it is just unreasonable.

Now, should contractors be required to recertify the need for an employee's clearance every 5 years? Is that a good idea to ask contractors to recertify the need for the clearance every 5 years?

General **Pauly**. I would support it.

Senator **Gore**. You would support it.

General **Pauly**. I would, indeed, Senator.

Mr. **Schwegler**. Senator, my observation would be, again, that's an alternative to working the problem. However, it's not at all clear to me that there would not be additional costs and attendant delay in the certification process, if that alternative was adopted. I would worry that it could become an administrative nightmare for both the Government as well as the private sector, but I would not discourage your subcommittee from actively looking at that, but let's understand what the ramifications of that kind of process might be in a reality sense.

Senator **Nunn**. I am not sure I understand, if I can pursue that, why that would be an administrative nightmare for the Government? If I understand what Senator Gore is asking, the contractors themselves, under his question, would be required to review the need for security clearances, presumably eliminating a large number of people, hopefully, that would no longer be required.

The Government itself is trying to struggle with a huge backlog of re-examinations. So to the extent you eliminate, by your own procedures, certain people from the need for classified status, that would reduce the Government's burden. Maybe I misinterpreted.

Senator **Gore**. That is exactly right. The first ones to be eliminated would be the 40,000 contractor personnel who never have any access to the material they are cleared to see.

Mr. **Schwegler**. Mr. Chairman, if I might, please?

Senator **Nunn**. Certainly.

Mr. **Schwegler**. My assumption was after the contractor executed that process internal to his own infrastructure, that the Government would then want to examine each of these recertification documents, which is the foundation, if you will, for what I say. If that assumption is incorrect, I withdraw my comment.

Senator **Nunn**. Certainly the Government could decide not to reexamine those you certified were not needed for clearance. Whatever you eliminate would be of benefit, it seems to me.

Senator **Gore**. It is a useful exchange, but it does not dissuade me from a feeling that has some merit. Would you like to give your comments?

Mr. **Welby**. On the recommendations, we concur, Senator. The only thing we question is the cost impact based upon the size of the plant site.

Senator GORE. You do think it might be a good idea?

Mr. WELBY. Yes, sir.

Senator GORE. According to the DOD report, and this has been brought out, Senator Nunn focused on this, about DIS will take a decade to perform the updates that are required just at the end of 1984, and I include in that the others they expect throughout the decade. In light of these constraints, what do you think about the idea of asking contractors to take some responsibility for some portion of the update process? For example, requiring personnel to complete an updated personnel security questionnaire every year. Whichever one wants to answer positively, go first.

General PAULY. I would have a reservation based on how the quality control of those investigations could be properly monitored by the governmental agencies that are required to have overall monitorship. I think I have a concern in that area.

Senator GORE. Well, the monitoring would involve, in part, when DIS gets around to this person for an update, then he has got a file to look at. Presumably, the amount of time might be contracted a little bit with the information available.

Do the other two witnesses share that concern?

Mr. SCHWEGLER. Senator, I would join General Pauly with regard to that concern, but I would further add, I believe the decision regarding a continuation of a clearance or the discontinuation of a clearance truly lies with the U.S. Government and not with the private sector.

Senator GORE. Any comment?

Mr. WELBY. I agree with that, Senator, because the contractor has no authority to suspend, deny, or revoke a clearance. I think the investigation should stay with the Government.

Senator GORE. What about a requirement on employees, on cleared employees to report all foreign travel? We have had several cases of people traveling to noncommunist countries to meet with spy masters. Would the requirement to report all foreign travel be helpful?

Mr. SCHWEGLER. Let me respond to that, if I might. We do have that requirement.

Senator GORE. You do have that requirement?

General PAULY. Likewise, Senator.

Senator GORE. Do you?

Mr. WELBY. Would you rephrase the question?

Senator GORE. All foreign travel not just to the communist countries.

Mr. WELBY. For all employees?

Senator GORE. Just cleared.

Mr. WELBY. Yes.

Senator GORE. You do. Both Mr. Boyce and Mr. Bell have told the subcommittee that some kind of coded imprint across classified documents that would sound an alarm if they were removed or improperly duplicated would have deterred them significantly. Do either of you have such a system and, if not, why not?

Mr. SCHWEGLER. Senator, if I might respond, please?

Senator GORE. Yes.

Mr. SCHWEGLER. Subsequent to the Boyce incident, we did install a system of magnetic metallic strips and the accompanying devices at entrances and exits of all facilities where we have SCI.

Senator GORE. I didn't realize that. That is very good. Does that system set off an alarm?

Mr. SCHWEGLER. It's an audible alarm; yes.

Senator GORE. What about the copying?

Mr. SCHWEGLER. If you are referencing the current 3M system——

Senator GORE [interposing]. Yes.

Mr. SCHWEGLER [continuing]. That's on the market, within the last few months, we began experimenting with that system at one of our facilities to become more knowledgeable about it.

Senator GORE. It is too early to tell whether you think it is feasible or not?

Mr. SCHWEGLER. Senator, that's correct.

Senator GORE. General Pauly?

General PAULY. We do not have such a system. The highest classification that we are currently operating on is secret, and we have not put such a system into being, although it sounds like it would be a good idea.

Senator GORE. Good.

General PAULY. I would support it basically, but I haven't done my homework because I just read about it in the handouts for this hearing.

Senator GORE. Good. We are making some progress here. Mr. Welby?

Mr. WELBY. Senator, I can't comment on the SCI area. I'm not involved in that directly, but at the Hughes Aircraft Co., we have not installed it but have had meetings with 3M people, as I indicated to minority counsel previously, and we are looking into it.

Senator GORE. What about the removal alarm?

Mr. WELBY. We're looking into it.

Senator GORE. You are looking at both the copying and the removal?

Mr. WELBY. Yes, sir.

Senator GORE. Bell and Boyce and Miss Schuler all had the same experience of walking out of the building with classified documents. My last question addressed this, but wouldn't a system of random searches of the cleared employees leaving classified areas—I haven't thought through the privacy implications, but they would seem to be enough to counterbalance the obvious legitimate interest in conducting such searches offhand, have any of you considered doing that?

Mr. WELBY. Senator, Bill Bell's testimony before the Nunn Committee indicated how he got in and out of the plant site with the documents. We had a previous policy of periodically inspecting briefcases, packages, et cetera, et cetera. As a result of the Bell case, all people now have to open their briefcases, et cetera. We do not allow wrapped packages to be brought into the plant site, Senator, without appropriate paperwork.

Mr. SCHWEGLER. Senator, my response would be that we do have a random search policy. This was instituted subsequent to the Boyce incident, one of the lessons learned, but let me quickly remind all of us that in the absense of having a metallic system, as I described such as we have for our own SCI work areas, if a person is intent on stealing a document, they are going to put it in their coat pocket. So it's a deterrent. I think it acts as an awareness raiser, if you will, all of which is positive, but it's not foolproof.

Senator GORE. I would agree with that. Did you have anything?

General PAULY. I will add the small-business dimension, if I may. Our plant is such that we are not the only people that occupy the two buildings that we're located in. So we have a problem staging something like that very effectively. Our security is based on the container itself, which is GAO approved; the awareness of the people and the attention of management, and that sort of thing.

Second, of course, I underscore, it is very difficult if someone wants to get something out to stop them without searching their body in some way because you can always strap things around you.

Senator GORE. There is just a very human problem here. When you have a group of employees coming in and out every day, the same people, you see them; it is just human nature that you are going to gradually diminish the level of scrutiny in these kinds of searches.

I hope it wouldn't become like the security system we have around here which is subject to the same sort of pressures. They try hard and do a good job. There is just a natural human tendency to get lax on it.

Mr. Chairman, I have some other questions that I would submit for the record. I would like to compliment this panel. I have learned a lot. Their responses have been very useful. Many of the exchanges, I hope, would indirectly wind up in our recommendations on this. I have learned a lot from this panel.

Senator NUNN. Thank you very much, Senator Gore. I want to thank each member of the panel for being here. Again, I know it is not the easiest thing to talk about it when you have had unfortunate experiences in your own company. I don't think any company in America is exempt from this sort of thing. It is a matter of where it happens and some of it is chance, some of it is beyond control, some of it may be controllable. We think all of you rendered a very valuable service.

Senator Gore, I am going to make a statement that concerns you on a particular news article. I want to thank each of you for being here. It has been very helpful. We would welcome your suggestions. If you think of any as we go along, we are going to have some suggestions which, I hope, we can agree on as a panel here. We are not a legislative subcommittee. We are an investigative subcommittee. We will be, I am sure, introducing some legislation as a result of this hearing.

General Stilwell has been so patient this morning and has been observing the proceedings going on. We are going to give him a unique experience to react to some of our suggestions before we finalize them when he testifies in a couple of weeks. So we will continue these hearings.

General Pauly, do you want to make any other statements?

General PAULY. I did, sir. I would want to add I will have some inputs for the record, with your permission, to clarify the issue of the circumstances of the Harper case and the part that SCT did or did not play in it.

Senator NUNN. Thank you very much. We will be delighted to have that.

[The information subsequently submitted for the record follows:]

Certain of the questions asked and statements made during the course of the hearing cause me to believe that a general misunderstanding exists as to what part Systems Control Technology (SCT) played in the Harper-Schuler case. The key point is that, having been formed in mid-1981, SCT was not in existance at the time the criminal acts were committed by Harper and Schuler. The company from which the documents were removed and copied was Systems Control, Inc. which was reorganized for other reasons in 1981 and certain of its resources were split out to create SCT as a totally separate company. The Systems Control, Inc. classified account was subsequently transferred to SCT. Of necessity, the FBI investigation involved SCT as well as Systems Control, Inc. because by the time of their investigation SCT had possession of the documents which had been compromised.

It is unfortunate that considerable confusion has existed because the names of the two companies are so similar; however, the FBI was extremely careful in preparing their case against Harper to insure that the proper distinction was made and all formal documents prepared in the case (such as the basic Criminal Complaint) identified Systems Control, Inc. as the company from which the classified documents had been obtained. Likewise, it is important that this distinction be properly recognized in the record of these hearings in the interest of correctness and clarity. This distinction also explains why I have not been able to fully respond to several of the questions which have been asked by the Sub-committee regarding conditions which existed at the time of the crime. I presume that a representative of Systems Control, Inc. could have responded more adequately.

[The prepared statements of General Pauly, Messrs. Schwegler and Welby, with attachments, follow. Responses of General Pauly, Mr. Schwegler, and Mr. Welby to written questions also follow:]

PREPARED STATEMENT OF GEN. JOHN W. PAULY

My name is John W. Pauly and I am Chief Executive Officer of Systems Control Technology, Inc. (SCT) of Palo Alto, California, having served in that position since June 1982. I have also served as Chairman of the Board of Directors over the same period.

I have been requested to testify before the Subcommittee concerning my views on the lessons to be learned from the James Harper espionage case, my judgment on the efficiency/effectiveness of the Defense Industrial Security Program and my comments on the recommendations of the Defense Industrial Security Review Committee. I have also been asked to provide the details of my company's security program. I am very pleased to have the opportunity to testify before the Subcommittee on this extremely important matter which is so vital to the security of our country.

Systems Control Technology was incorporated as a separate company on 12 July 1981. It was organized from two of six operating divisions of Systems Control, Inc. (SC) also of Palo Alto, a company which had been formed in 1968. The overall company had been involved in computer-aided analysis, software development and systems engineering work, serving both government and commercial clients, with certain of the government contracts requiring classified work. With the purchase of Systems Control by the British-Petroleum Group in 1981, the defense-related business was split off into the separate company which was organized under a Proxy Shareholder agreement in compliance with Department of Defense directives. At that time, SCT was physically separated from the original company, was restructured and began operating under a substantially different set of rules under DOD cognizance. The individuals selected as proxies represented a wide range and great depth of both government and non-government experience. My first association with SCT was as one of those proxies.

My prior experience had centered around a 35-year career in the United States Air Force from which I was retired in the rank of General in 1980. At the time of my retirement, I was serving as the Commander-in-Chief, U. S. Air Forces in Europe and, in the NATO structure, as the Commander, Allied Air Forces in Central Europe. Immediately prior to that I held several operational and planning positions within the Joint Staff and the Air Force. For virtually all of my military career I was required to deal with classified matters on a daily basis and to use and protect documents at all levels of classification. I believe that it is fair to say that this type of experience develops a unique sense of security awareness and security discipline which I have maintained at SCT. I hasten to add, however, that, at my first contact with SCT, I was very favorably impressed with the security consciousness which I found throughout the company.

The Harper Case

Upon the departure of my predecessor to accept another position in the summer of 1982, I became the CEO of SCT. Approximately nine months later, in March 1983, the Federal Bureau of Investigation contacted both companies (SC and SCT) to solicit our help in an espionage investigation which involved the passing of classified documents to the Polish Intelligence Service several years before. The suspect was James Durward Harper, Jr., but it could not be determined how he had obtained the documents in question since he held no security clearance himself. The FBI had determined that his wife had worked for an officer of Systems Control some time before and had held a security clearance during the period in question. Therefore, it was necessary to establish whether she had had access to the type documents known to have been compromised. Both companies offered to cooperate fully; however, since the classified account and the classified documents had been transferred to SCT when it was formed, most of the investigative support was provided by my company. This was accomplished on a very "close-hold" basis with only one of my Division Managers, Dr. Kenneth M. Kessler, and myself involved. We supported the FBI for several months and were ultimately able to identify a number of documents which matched the material passed to the Poles. These documents had been illegally duplicated and the copies provided to the Polish Intelligence Service. The FBI was able to prove conclusively that James Harper had, at one time, had temporary possession of these documents. Harper was taken into custody in October 1983 and was charged with espionage and tax evasion. He was subsequently sentenced to life in prison.

As was developed during the investigation and trial, Harper acquired possession of the documents through his wife (then girl friend), Ruby Louise Schuler, during the 1979-1980 time period. Schuler had been employed by Systems Control as the secretary to an officer of the company at that time. She was properly cleared by DOD for classified national defense information up to and including the SECRET level. In order that she could assist her supervisor on the projects on which he was working, she was properly authorized access to his safe which contained the classified documents later compromised. As would later be proven, Schuler would systematically remove documents from the safe as she closed the office for the evening, covertly take them home in a briefcase, handbag or strapped to her body, copy them on a duplicating machine at home and return them to the safe when she arrived for work early the next morning. Negotiations had begun by Harper with the Poles in May 1979 followed by a series of meetings in various locations in which a portion of the copied documents were turned over. The remainder were later recovered. The last reported delivery was made in April 1981, and Harper received approximately $250,000 in total payments. Louise Schuler retired from Systems Control in August 1981 and died of natural causes in June 1983.

After a case such as this, it is imperative that all possible steps be taken to identify what lessons can be learned from the experience and to take the corrective action indicated. To do this it is necessary to seek out the root causes or the weaknesses in the security program which permitted this breach to happen. I cannot testify personally to the conditions which existed since I had no contact with Systems Control at the time, nor have I ever met or seen Schuler or Harper. I can, however, make some observations that are pertinent. Most importantly, it must be noted that Systems Control was provided a security clearance by the Department of Defense in 1968 having fully met the criteria for the granting of such a clearance. This meant that the facility met certain required standards, that necessary security policies and procedures were in force, that employees had been educated in security requirements and that classified information could be properly protected. Through the years Systems Control was subject to regular inspections by the appropriate DOD agencies (now the Defense Investigative Service). That they were permitted to retain their facility clearance testifies to the fact that they were found to have had an effective security system throughout the period. Conversations that I have had with several individuals who were employees of that company in the late 1970s tend to verify that the security program was respected and effective.

Unfortunately, all security programs designed to protect classified national defense information are heavily dependent upon the integrity of those individuals who the government, after thorough investigation, clears for access to classified information. In this case, Schuler had been cleared for access to information up to and including the SECRET level. She betrayed that trust without detection and, therefore, the entire security system broke down. Once a properly cleared person decides to turn against his or her country it is extremely difficult--if not impossible--to prevent compromise of defense information.

This introduces another dimension which was prominent in this case. It is the absolute necessity for all personnel to be constantly alert to any manifestations in their co-workers actions which would hint that they could be a security risk. In this case Schuler was known to be a heavy drinker and some have classified her as an "alcoholic." She was known to have carried a bottle of whiskey to work regularly in her purse. To be sure, the danger signs were there although no one recognized them to be serious enough to constitute a potential security problem. If I were to identify a "lesson learned," this would be it.

Defense Industrial Security Program

Despite certain recent compromises such as that seen in the Harper case, I believe that the Defense Industrial Security Program is highly effective within the resources that have been allocated to the agencies involved. It provides a broad and solid structure for the accomplishment of its monumental task. I find the DOD Industrial Security Manual for Safeguarding Classified Information to be an excellent, yet bulky, documentation of a program which is designed for both large and small defense companies alike. It provides all of the detailed policies and procedures necessary to make the program work in a rational way. The overall program itself attacks the problem from every dimension possible, including physical security, education of our people in security awareness, clearance procedures for those requiring access to classified material as well as clear policies and detailed procedures for protecting the classified documents themselves. Finally, its inspection system, which is part of the program, provides an excellent mechanism for the Defense Investigative Service to properly oversee the program and to assure that all defense contractors maintain the required degree of security under dynamic security programs of their own. I must add that I find the DIS structure in the field to be extremely helpful in an advisory role as well, assisting companies confronted with complicated security problems or providing interpretation of published directives.

Having commented positively about the Defense Industrial Security Program, there is no question that it could be strengthened with the commitment of additional resources to the task. Certainly such things as more frequent contact with defense companies, more frequent interaction with the employees and more frequent updates of security clearances would go a long way toward improving the program. I believe we should look at the lessons learned in the recent compromise cases and apply additional resources to correct the weaknesses which have surfaced in these cases. To me the first crying need is to tackle the human reliability aspects. The integrity of the people cleared is intended to be the keystone of the entire security program; instead it appears to be its "Achilles' heel." This fact certainly indicates that priority attention should be applied here. It would follow that such things as updating SECRET clearances on a realistic cycle, reducing the number of people who hold active clearances and controlling the number of people having a need-to-know would go a long way toward improving the situation. To be sure, the recommendations of the Defense Industrial Security Review Committee have addressed these points squarely.

SCT Security Program

Since our incorporation in mid-1981, the SCT security program has been maintained under and tailored to the DOD Industrial Security Manual for Safeguarding Classified Information. We conform to the policies and procedures outlined in that document and fulfill the many specific requirements which this manual levies upon us. Our managers and employees take security seriously, and, as mentioned earlier, from my first involvement with SCT, I have been very favorably impressed with the security consciousness that I have observed. This security awareness is relatively easy to recognize in a small company of some 160 people in which you interface with a significant percentage of the employees on a daily basis. Having spent most of my years in the military, I was curious as to what I would find in the day-to-day operations of a high technology defense contractor. I was pleasantly surprised! My objective from the outset was to improve our program even more although the measures that we have taken in general have been in the category of "fine-tuning" as opposed to sweeping changes. A good percentage of these were based on corrections to minor deficiencies observed by Defense Investigative Service inspectors.

The SCT Security Program itself includes provision for all facets of the wide area of security tailored for application to a company of our size and the physical facilities from which we operate. It deals with such subjects as facility security, visitor control, employee identification, obtaining authority for access to classified material, control and protection of classified documents, security education and computer security. SCT has published a company Security Guide which promulgates and amplifies the guidance contained in the DOD Industrial Security manual for specific application at SCT. This document is designed to serve as the day-to-day security reference for use at SCT containing only that portion of the DOD manual which is pertinent to SCT. Management and security personnel are active in fostering the formal security program. Security issues are discussed regularly at scheduled corporate management meetings, frequent "walk-throughs" of work areas are conducted on a daily basis to observe security practices, self-inspections are held periodically and the subject of security is raised at every appropriate opportunity in the day-to-day conduct of business.

Although SCT as a company was not involved in the Harper case, we have reacted positively to the lessons learned in that case in an effort to strengthen our security. Of particular interest were an emphasis on proper procedures for entering the facility during non-duty hours and highlighting the responsibility of all employees to report any adverse information they may have on any employee having access to classified information. Additionally, at the time that the Proxy Shareholders were advised of the ongoing Harper investigation, they directed us to conduct a thorough examination of the entire SCT security program, although the compromise had occurred before our company was formed. This detailed self-examination did not reveal any specific weaknesses. The Proxies also forwarded a letter to the Federal Bureau of Investigation to insure that the FBI had been receiving total cooperation from SCT and to request the impressions gained by their agents as to the status of the security being maintained within the company. The Bureau confirmed that they had received outstanding cooperation and, at a meeting with our Board of Directors, the agent in charge of the case stated that the security he observed during the investigation was as good as he had seen in the industry.

Defense Industrial Security Review Committee

I have reviewed the recommendations of the Defense Industrial Security Review Committee and enthusiastically agree with the great majority of them. I am impressed with the thoroughness in which they examined the problem and the wide focus and breadth of the recommendations they have made. To be sure, certain of these recommendations will require additional funds and further commitment of resources, but the problem is a serious one and, if the expected payback on specific recommendations would significantly foster the desired security, it should be supported.

Although I am in general agreement with most of the recommendations, I particularly support the following:

(a) the need to repeat and update all necessary checks for SECRET clearances

(b) the need to place more emphasis on the human reliability dimension of the problem

(c) the need to revise the format of the Industrial Security Manual to eliminate much of the detail

(d) the need for all cleared employees to report all foreign travel

(e) the need to expand the DOD security inspection rating system to award one of four ratings (Superior, Satisfactory, Marginal or Unsatisfactory)

(f) the need for DIS to provide a more formal certification/accredation training program for contractor industrial security personnel.

The recommendations with which I do not concur include the following:

(a) the proposal to create separate advisor and inspector roles of DIS representatives. I believe in the long run this separation would be counterproductive. As a small company, SCT appreciates the free two-way dialogue we have established with DIS which continues through the inspections themselves. It is helpful to us and I believe a definite advantage to our efforts toward better security. The "adversary role" created by having separate inspectors may not be as productive overall.

(b) the proposal to establish a national Industrial Security Hotline Program. I believe that such a hotline would be subject to tremendous abuse. Whereas hotlines regarding establishments within the government might be effective, such communications regarding individuals could not only vent prejudices but also ruin individuals' reputations unjustly. If an individual is certain enough that he or she has a reasonably valid comment, he or she should be prepared to use the normal, established channels of reporting the information.

Subject to the specific comments listed above, I concur generally with the recommendations of the Committee. They appear to have examined every possible aspect of the problem, and I believe that most of the recommendations will have a positive impact on our efforts to improve industrial security.

Attachment A

WRITTEN RESPONSE
by
GENERAL JOHN W. PAULY, USAF (RET)
SYSTEMS CONTROL TECHNOLOGY, INC.

Q. Both William Bell and Ruby Schuler had secret clearances based only on a National Agency Check. Bell claimed his secret clearance hadn't been updated in 28 years. Should the present investigative scope of secret clearance be expanded? How?

A. In my judgment it is imperative that secret clearance investigations be updated on a five-year cycle similar to top secret clearances.

Q. A review of the DOD Industrial Security Inspections for your company indicated "good" security with only minor deficiencies until Harper's arrest on October 15, 1983. The next inspection, in December 1983, found "poor" security and "major deficiencies." Could you explain this apparent inconsistency? Were the inspections prior to Harper's arrest erroneous? Were they pro forma and not in depth? On the other hand, was the December 1983 investigation unfair and/or biased? Or, did the security at your firm deteriorate significantly from May 1983 to December 1983?

A. The December 1983 security inspection conducted by the Defense Investigative Service differed substantially from normal semi-annual inspections. It was called an "Enhanced Inspection," and was conducted by the senior inspectors from the national, regional and local levels of DIS. This intense inspection lasted two full weeks as opposed to the normal 3-4 days. At the outbrief I was told that SCT was rated "Satisfactory" but that two major discrepancies had been observed. These were instances in which basic procedures for the proper safeguarding of classified information were not followed.

In my judgment, there is no inconsistency here. This inspection, being more thorough, made more observations over a longer period of time and, therefore, more discrepancies were noted. I also believe that the two instances noted were partly happenstance and did not reflect the true security situation at SCT at the time. It is my opinion that DIS agreed with this assessment. The December 1983 inspection was not unfair or unbiased and, in fact, the security at SCT had not deteriorated between May and December 1983.

Q. What have you done to remedy those deficiencies revealed in December 1983?

A. The major discrepancies noted were investigated thoroughly (one of them by me personally) and those personnel found at fault received verbal reprimands. Additionally, the facts of the incidents were briefed throughout the company as "case studies" so that others would learn from the mistakes. Finally, our procedures and awareness programs were both reoriented somewhat to put more focus on the pitfalls involved.

Q. Do you feel that present government policy should be changed to permit the granting or continued holding of a security clearance to be a condition of employment?

A. If working with classified material is part of the duties of a given position, I see no logic in not making the holding of a clearance arequirement just like any other capability. I, therefore, would strongly support such a change.

Q. Do you feel that contractor security personnel should have access to the privacy portions of clearance applications?

A. I feel strongly that that information should be available to contractor security personnel.

Q. The DOD report found that "DOD mandated and contractor initiated physical and personnel security controls during nonworking hours, to the extent they exist, are generally weak and ineffective, and as such provide inadequate protection against unauthorized access or removal of classified material."

In both the Boyce and Harper cases documents were removed after hours in the absence of any effective controls. General Pauly, what after-hours controls existed at the time of the Harper case? What is the situation today?

A. I have no knowledge as to the after-hours controls which were in effect at Systems Control, Inc., at the time the documents were removed by Louise Schuler (Harper case). At the present time at SCT, the buildings are locked by key and the individual interior work zones within each building also require a key to gain admittance. All classified containers are located within these work zones. A sign-in register is maintained at the main entrance,

Q. Should DOD require security controls be enhanced during nonworking hours at cleared Defense contractors authorized to store classified material on the premises?

A. I can only respond to that question in the context of the smaller companies. In this regard, I do not believe that SCT's current security controls for nonduty periods require enhancement. Virtually all of the security of classified material is provided by the containers themselves and the security awareness of the employees. Additional measures beyond those presently in effect would not significantly improve the security situation during off-duty hours. For example, it would not prevent a properly cleared person from illegally removing classified material as in the Harper/Schuler case. Only a briefcase search and a personal search would have prevented that crime.

Q. General Pauly, in the November 1982 inspection, SCT was cited for improper retention of classified documents. In May 1983, SCT was again cited for improper retention of classified documents. According to the FBI, some of the documents which Harper and Schuler compromised to the Poles were improperly retained at SCI, the predecessor for your firm, SCT. What improvements have been made on retention of classified materials at SCT? What incentives do a contractor like SCT have to respond to repeated security citations by DIS?

A. SCT has compiled a computerized listing of all classified documents in our possession correlated with the individual contract which authorizes such possession in each case. When that contract is completed, a printout is issued which directs the project leader to dispose of the applicable documents or to submit a request for waiver of the retention rules. A follow-up system is designed to insure that this procedure is effective.

A. With regard to incentives to insure against repeated security discrepancies, the principal deterrent is the threat of losing the company's facility clearance. This action could be taken by DIS in cases where they feel that the contractor is not sufficiently motivated to correct reported discrepancies.

Q. In each of three cases which you are familiar with, the William Holden Bell case at Hughes, the Harper-Schuler case at SCT, and the Christopher Boyce case at TRW, extensive classified information was lost. Yet in none of them were the contractors themselves held accountable in any way for the breaches in security. No fines were levied, no disciplinary action was taken, no contracts were lost. Critics of the current system say that is wrong, that contractors should be held accountable for security failures. If the contractors were held accountable to some extent for the conduct of their employees, might that not result in increased security in the defense industries?

A. First, let me again point out that the Harper-Schuler case did not happen at SCT. It happened at Systems Control, Inc. several years before SCT was formed.

Although I have some sympathy for the notion that contractors should be held accountable to some extent for serious breaches of security, it does not appear appropriate in cases where properly cleared individuals willfully compromise classified information or documents. In these cases it appears that the government would bear considerable responsibility since the Defense Department investigates individuals and grants their clearances. Additionally, it is the government which establishes policies on reinvestigation, etc., which are directly relevant in such cases. We must remember that it is the lack of integrity of cleared individuals which was the major cause of all of the recent espionage cases.

Q. In your opinion, what is the biggest problem with our current personnel security program?

A. In my judgment, the biggest problem in the DOD personnel security program is that there is no way to insure the personal integrity and loyalty of all cleared personnel. This is the area in which we should focus our attention in our efforts to strengthen the personnel security program.

Q. Do security protection standards for the handling of classified material vary between government and industry? If so, does this pose a problem to industry?

A. Security procedures, rather than standards, do differ somewhat between government and industry because of differences in the percentage of the work which is classified, differences in overall security protection, the existence of an added discipline level among those in government services, etc. I do not consider that this variance generally poses a problem to industry.

Q. Should DIS establish a nationwide security hotline for receipt of anonymous information (6(b)(1) of the Industrial Security Manual) impacting on the Defense Industrial Security Program?

A. Answered in my direct testimony.

Q. Should the inspection rating system be changed from satisfactory/unsatisfactory to a graded system such as outstanding, superior, satisfactory, marginal, and unsatisfactory?

A. Yes, such a change would let contractors know how effectively they are complying with government security regulations in a more definitive way. Additionally, it would permit these inspections to provide contractor management with a more effective management tool.

Q. In many "carve out" or "black" contracts an award provision for security is utilized. What are your feelings about such a proposal for Secret and particularly sensitive DOD contracts?

A. Although I support such a notion in principle, I do not believe it to be practical since government clients would have great difficulty in measuring the effectiveness of the security program as it applies to their project.

Q. Contractor indoctrination generally covers the prohibition of unauthorized removal of classified material from the company. Should more specific measures be established to prevent personnel from bootlegging classified material from employer to employer? If so, what do you do to prevent this?

A. In addition to incoming indoctrination, individuals, when leaving a company, are required to sign a certificate that they are not taking any unauthorized material with them. Needless to say, however, this certificate is only a passive measure and cannot be expected to inhibit bootlegging to any significant degree. The only suggestions I would have would be to strengthen controls on the duplication of classified material and to make the recruiting company responsible for seeing that no unauthorized classified material is introduced and stored within their facilities.

Q. Should full-time DIS representatives be assigned to contract facilities, as recommended by the DOD Harper Report?

A. Such a measure may be helpful in the facilities of the larger defense contractors; however, I do not believe it would be justified manpower-wise in the smaller companies of 1000 or less employees.

Q. Do you have any recommendations for legislative action which would enhance personnel security?

A. My primary recommendation for legislation would be to require that persons with SECRET clearances be reinvestigated on five-year cycles. The manpower resources to support this additional requirement, of course, must also be provided.

Q. General Pauly, in view of the lessons learned in the Harper case, has your company enhanced its personnel and physical security program?

A. As you know, SCT provided a great deal of support to the FBI during their investigation of the Harper case. During this process we became acutely aware of the details of the criminal acts committed. This knowledge has been very helpful to the management and security personnel of the company in strengthening our own personnel and physical security program. Numerous measures have been implemented as a result of the knowledge gained.

Q. General Pauly, what new personnel and physical security requirements has Systems Control Technology implemented since the Harper case?

A. The SCT personnel and physical security program is constantly being strengthened and improved in an effort to provide the best possible security. Those measures taken since the Harper case include the following:

As part of our employee security education/awareness program we have prepared and distributed a handy, bound brochure containing the key information on security regulations.

Emphasis has been placed on the use of the weekend sign-in log for visitors.

Frequency of checks of all classified containers in the company has been increased to twice per day.

The SCT Security Department staff has been upgraded in number and the Security Officer has attended the DIS Management Training School.

Security issues are regularly highlighted in weekly SCT Management Meetings.

Finally, I tour the entire Palo Alto facility at least once each day for the purpose of checking the general security situation within the operating offices.

Q. General Pauly, do you think that your present security system would have prevented the Harper compromise? Please explain how it would have done so.

A. Although I consider our present security system to be a strong one, I do not believe it would have prevented the Harper compromise. In my judgment, the only way to absolutely prevent individuals from removing classified documents from the premises would be to maintain a constant guard force at all exits and to require the search of all briefcases as well as some form of personal search to insure documents were not strapped to an individual's body. I do not believe this to be practical.

Q. General Pauly(SCT), prior to the Harper/Schuler case, did Systems Control Technology have an effective security education awareness program?

A. Since SCT did not exist at the time the Harper/Schuler crime was committed, I am unable to respond. I have no knowledge as to whether the involved company, Systems Control, Inc., conducted an education awareness program; however, in view of regular DIS inspections I would assume that such a program was in force.

Q. Would you furnish a copy of the number of 6(b) violations reported by your company for the last five (5) years?

A. Since SCT was incorporated in 1981, one report has been submitted under paragraph 6(b) of the Industrial Security Manual. These are reports of adverse information rather than "violations" per se.

PREPARED STATEMENT OF PAUL W. SCHWEGLER

TRW is pleased to provide information to the Senate Permanent Subcommittee on Investigations on TRW's security procedures for special security programs, changes and improvements made as a result of the Boyce case, and some of the recommendations of the DOD Industrial Security Review Committee.

First, perhaps it would be helpful to outline the procedures followed at TRW in dealing with the security aspects of a typical special security program.

When the Department of Defense or the intelligence community solicits TRW to bid on a program with special security requirements, the request is brought by courier to the Director of Security, Health and Safety, the principal point of contact. The request is delivered in the form of a request for proposal (RFP) -- a solicitation by the Government for the company's participation in a study or other activity.

After the company has made a decision to bid, a senior security manager meets with the program manager who has been selected to manage TRW's proposal to the Government. Working with the program manager, we then select those individuals who will participate in the program. They are personnel from the various scientific, engineering and other disciplines who will perform the work necessary to the program. We also select administrative personnel such as management specialists, pricing and contract specialists, security clerks, reproduction personnel, telex operators and secretaries.

The names of all of these management, engineering and support personnel initially selected to work on a special security program, although they may have had a previous special security access, are submitted to the Government for their consideration with respect to the granting of an additional security access appropriate to the specific program. The responsibility and duty to clear and approve personnel for a special security program rests with the U.S. Government. After we submit to the procuring government agency the names of those individuals who will have the "need to know" in connection with the program, the Government investigates and approves or disapproves each person's access to this activity. .

Once approved, each individual is briefed in depth by approved security personnel with regard to his or her security obligations. This briefing includes type of activity or project, special security requirements, project access requirements, and physical location restrictions. A record -- called an access control card -- is kept by TRW on each individual who was briefed on a specific special security program. In addition to the briefing, there is a system to provide formal introductions of participants in the program. This ensures that there is a clear mutual recognition of those involved who have a need to know.

We consider TRW's security practices relating to personnel, documents and physical security to be rigorous and exact. While the briefing process just described is one that applies specifically to individuals selected to work on special security programs, these individuals (along with all other TRW employees) would also have received security briefings as part of their initial processing and orientation -- beginning on the first day of their employment at TRW.

During our new-hire orientation, we outline the penalties for violation of the espionage statutes and discuss classification levels including confidential, secret and top secret. There is a discussion of the need-to-know requirement for access to classified information and of the proper procedures for storage and handling of classified information. This is repeated for each new or additional clearance. Each new employee is given a TRW booklet containing excerpts from the U.S. espionage statutes, which the individual is required to read.

All new employees must sign a security briefing statement before being allowed access to any classified information. The statement reads: "I will not knowingly and willfully communicate, deliver or transmit in any manner, classified information to an unauthorized person."

A second briefing -- the Security, Health and Safety Orientation -- is also given to each new employee. During this briefing the individual is again advised of his or her responsibilities when given access to classified information. The employee is shown examples of espionage activities engaged in by foreign countries to obtain classified information.

In addition to the personnel clearance and briefing process, we have comprehensive document security procedures. All documents generated or received in special security programs are identified by control cards. Each document is assigned a document control number. If a copy is made of the document, a copy number is assigned and that number is recorded on the card. The control card includes the name -- usually shortened -- of the project, date of generation or receipt, the number of pages, and the distribution. Security classification and classification authority are recorded on the top and bottom of each page of the document.

Documents transmitted to the government agency responsible for the project are wrapped and then double-wrapped in large envelopes. They are logged on a manifest and then hand-carried by a two-person courier team to the designated government agency representative.

When a document is to be destroyed, a formal document is prepared -- a document destruction card -- certifying that the document is to be destroyed. The documents are transported by two TRW armed guards -- with the required security clearances -- to an authorized location for document destruction. The guards witness the destruction, which is by a pulverization process.

With regard to physical security, we fully comply with the Government's requirements for Special Compartmented Information Facilities (SCIF) and the Defense Investigative Service Program (DISP). This includes protection of SCI and DISP material by building structure, access and communications security.

In the design of buildings, we meet all special physical requirements for vaults and work areas in selection of materials, including thickness of walls, and electromagnetic shielding.

Access to facilities is controlled by our own security force trained to protect Government and company assets and people.

They are fully trained in Government regulations for security, as well as health and safety concerns such as cardiopulmonary resuscitation and general first aid. Supporting the security force is a state-of-the-art technical backup system including alarms for fire and intrusion, and a closed-circuit television system.

The security force, with an average company tenure of 7 years, possesses the various levels of clearance necessary for their job assignments. For both SCIF projects as well as DISP classified programs, the security force is responsible for individual identification to permit access to closed areas only to approved personnel.

Communications security requirements are dictated by the National Security Agency, as well as other intelligence agencies. They also furnish the equipment and approve personnel to be used.

While procedures relating to personnel clearance and briefing, document security and physical security are critically important deterrents, they cannot ultimately guarantee security. Sound security procedures are essential, but in the final analysis it is the individual's personal integrity and loyalty to our country that provides this guarantee.

It is in this context that we address the case of Christopher John Boyce, who was hired by TRW as a general clerk on July 29, 1974. Boyce was employed at TRW for approximately two and a half years until he terminated his employment on December 17, 1976.

During his employment with us he received three security clearances from the U. S. Government. In accordance with standard procedures, he was granted a confidential clearance on the day he was employed, a secret clearance from the Department of Defense on September 27, 1974, and a top secret clearance from the Central Intelligence Agency on November 15, 1974. Boyce received the new-hire security briefings I described and, since he was selected to work on programs requiring special security measures, he also received the special security briefing described earlier and a reorientation briefing during which he again signed an oath not to divulge classified information.

Since TRW's inception, more than 75,000 employees have gone through similar clearance and briefing procedures. These procedures are thorough and proper. Other than Christopher Boyce, not one of the other thousands of people has -- to our knowledge or that of the Government -- ever committed treason against our country.

We are glad to outline some of the lessons learned from the Boyce incident, but we would emphasize to you that the case is now more than eight years old, and the intervening years have brought improvements in security practices and procedures as well as improvements afforded by technology.

We also recognize that Mr. Boyce is testifying before this Subcommittee. While we hope that Mr. Boyce at long last feels some remorse for his crimes and provides the Subcommittee some unique insight on the important issue of industrial security, we must also point out that after weeks of testimony at the trial where he was convicted of espionage, Judge Kelleher said, "The Court didn't find any veracity in him... The Court didn't believe a word the defendant expressed on any material issue."

Despite our view that our security procedures were sound prior to the Boyce case, the investigation performed by the U. S. Government immediately following the arrest of Boyce revealed that at that point in time there were a limited number of variances to the Government requirements. They included a very small number of alarms which were not operational, the need to require procedures for sequential prenumbering of blank badge stock and to upgrade cabinets which did not meet GSA standards, some limited evidence (discovery of two empty half pint bottles) of the use of alcohol on the premises, and a conclusion that Boyce's immediate supervisor had been weak -- evidenced in part by Boyce's alleged long lunch hours.

On April 28, 1977, Boyce was convicted of espionage involving the transmission of top secret information obtained from a special security program to the Soviet Embassy in Mexico City. On September 12, 1977 he was sentenced to 40 years in prison.

In addition to the Government's investigation, we engaged in a self-analysis to see what we could learn and to improve the overall effectiveness of TRW's and the nation's security program.

As a result of these reviews, we made the following changes on our own to enhance the protection of highly sensitive Government information in special security program areas:

- Employees' briefcases, purses and packages are now subject to random searches, and right-to-search signs are posted.

- Magnetic metallic strips are affixed on all documents and detection devices are located at building exits. An audible alarm sounds if an individual attempts to carry such a document through an exit.

- By use of a combination of coding on each employee's special access badge and a digital code entered by the employee, a registry computer identifies employee access authorization and records the time and date of each entry. This system supplements the primary access control, which is face-to-face identification by security guards.

- Independent TRW security audit teams review security systems and purge document holdings.

- "Satellite" reproduction machines were eliminated and were replaced with central reproduction facilities, with two-person operation required.

- We intensified our security awareness and motivation program for all employees. This program ranges from special guest lectures (FBI, Secret Service, DEA and others) to a wealth of internal communications tools: posters, videotapes, security reminders in travel packets, disposable coasters, a Security Awareness Week, "how to" booklets, and security recognition awards, as well as use of the company newspaper to promote security awareness. Our program of audits and inspections also helps to keep security awareness high.

As a condition of acceptance to an SCI job assignment, by TRW policy each employee must:

- Sign an authorization statement as a condition of assignment to any special security program. This authorization enables the Government to obtain information about an individual's finances, personal affairs and prior employment.

- Inform security of any foreign travel plans -- not just denied area travel -- and participate in a detailed debriefing on return, when requested. Failure to comply with this requirement constitutes a security violation. (This applies also to DISP.)

In addition, at the Government's request, TRW agreed to make arrangements for employee participation in polygraph examinations, administered by the Government, for those individuals in sensitive positions providing broad access to classified information. These polygraphs are administered upon assignment to such sensitive positions and randomly thereafter. At TRW, submitting to a polygraph examination is a condition of assignment, not a condition of employment.

Following the Boyce case, the Government also initiated a series of industry-wide practices to enhance the protection of SCI programs:

- Industry-wide inspections for compliance to all SCI regulations.

- Security management seminars to educate management as to requirements for SCI programs.

- Incentive fees on contracts based upon security performance.

The following standard practices for special project communications, registry, reproduction centers, and courier operations were adopted by TRW on its own and recommended to the Government to be standard industrial practice. The first two have since been adopted throughout industry.

- Double-keying -- Two persons must open and close doors in such secure areas. Both individuals must sign a validated registry sheet. A list of authorized names and signatures is maintained by the security guards.

- A two-person policy applies in all such special access areas, meaning that no employee in these areas ever works alone.

- Security personnel working on special security programs are routinely rotated to different parts of the project or other projects, and different physical locations every six to nine months.

In addition to the changes we made ourselves, our comprehensive review led to recommendations, made through the CIA, that the following security practices be adopted industry-wide:

- Personal history statements should be augmented to require the names of five "leisure-time" associates. (The Defense Investigative Service now requires that one such individual be listed.)

- Open shelf storage in special program communications, registry and reproduction vaults should be eliminated. (This recommendation was adopted.)

- Special program communications facilities should be consolidated and communications centers should be staffed by Government personnel. (The recommendation for consolidation was adopted.)

- A two-person procedure should be used when special security material is carried by courier. (This recommendation was adopted.)

Finally, you have asked that we comment on the Report of the DOD Industrial Security Review Committee. Many of the recommendations address internal Government procedures on which we have no comment. However, we do offer the following for your consideration:

- We would recommend expansion of the existing investigative criteria presently used to grant secret clearances. And, we believe the national agency check should be augmented in some manner. For example, a recent change in Top Secret clearance procedures requires an interview with the candidate; this might also be considered for granting a Secret clearance.

  We would, however, be concerned about any change that would lengthen the clearance process because any additional delay slows program performance and increases costs to the Government.

- Although the need-to-know principle is effectively applied in special security programs, it should be more strictly enforced in dealing with all other types of classified information, both in industry and Government. Information should be provided only to personnel who have an established need.

- A uniform security motivation and awareness education standard should be established for industry and Government. Greater attention should be given to the security awareness and motivation programs for all personnel possessing a clearance and having access to classified information. TRW has developed such programs.

- A standard set of minimum security regulations in non-SCI areas, applicable to government contracting in all Federal agencies, should be developed covering the entire spectrum of Government-imposed security requirements and guidelines.

- A Government-wide adjudication process that is well understood by both the public and private sectors is needed. The adjudication process should be strengthened to include more effective means for removal or denial of clearances.

In conclusion, we believe that TRW has a sound and effective security system. However, we know from past history that no security system is invulnerable and therefore we must never become complacent.

We are proud to state that TRW has received the James S. Cogswell Award five times in 18 years, most recently in 1982. This is the senior security award conferred by the Department of Defense's Defense Investigative Service. The recognition is for "sustained outstanding implementation of the Defense Industrial Security Program thereby contributing significantly to the security interests of the Nation."

We are determined to maintain this high tradition at TRW.

RESPONSES

TO

ADDITIONAL QUESTIONS

OF

SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

Submitted by

Electronics & Defense Sector
TRW Inc.
Redondo Beach, California 90278

May 10, 1985

Q. Both William Bell and Ruby Schuler had secret clearances based only on a National Agency Check. Bell claimed his secret clearance hadn't been updated in 28 years. Should the present investigative scope of secret clearance be expanded? How?

A. We are unable to comment on the Bell or Schuler case. As a general principle, we would be supportive of expanding the investigative scope provided that it doesn't lengthen the clearance process. A lengthening of the process delays vital national programs, and has the effect of increasing costs to the government when employees cannot work on programs to which they are assigned pending clearance.

Greater emphasis on peer relationship investigations would be valuable, as one example. And, as we mentioned in our written testimony, a recent change in Top Secret clearances requires an interview with the candidate. This might also be considered for granting a Secret clearance.

Q: Hughes Aircraft, as a result of the Bell case, invoked a system of searching all packages going into and out of their facilities. Why hasn't TRW done so in light of the Boyce case?

A: Since the Boyce incident, we instituted a policy of random search of briefcases, purses and packages, and have posted right-to-search signs in sensitive compartmented work areas. These serve as deterrents and raise awareness. We believe that this, in combination with the use of magnetic metallic strips on SCI documents and our application of the two-person policy described in our written statement, is an effective combination of procedures that accomplishes the same goal as mandatory searches.

Q: If Mr. Boyce applied for a job today with the background he had in 1974, would he be hired? If not, why not?

A: Mr. Boyce alleges he was hired and cleared because of his father's friendship with TRW's Mr. Regis Carr. We should first distinguish between hiring and clearing.

As in most organizations, an introduction and qualified references enhance the prospects of a job offer, provided the individual is qualified for the position available. So it may be fair to say that this friendship, dating to a period when both were FBI agents, had a favorable influence on Mr. Boyce being selected for a job. Nevertheless, it must also be said that Mr. Boyce was qualified for the position that he accepted as he met all of the requirements of the job description.

However, the hiring process has no bearing on the clearance process. After being hired and then selected for sensitive positions, the usual applications were submitted for the Government to investigate and clear Mr. Boyce for classified programs. The Government, not the contractor, has that responsibility.

In our written statement, we commented that investigation of leisure time associates might have raised a "red flag" as to Mr. Boyce's suitability for receiving a clearance. We recommended to the Government following the Boyce incident that greater emphasis on interviewing peers would be beneficial.

However, Mr. Boyce's suggestion that informal inquiries by company personnel should have been made is based on false information and shows a lack of understanding of clearance procedures. For example, Mr. Boyce indicated that, if Mr. Regis Carr had queried his own sons, whom Mr. Boyce called his "high school classmates," they could have "easily told him far more than the government's entire background investigation did." The facts are that Mr. Carr's sons and Mr. Boyce were not classmates, were in different grades and in different high schools; in fact, they associated with completely different circles of friends.

We would also emphasize that the Government's Industrial Security Manual prohibits employers from requesting pre-employment security clearances, and that there are many legal barriers which prevent contractors from obtaining private and personal information in the hiring process. Based on all of these considerations, today's procedures might not have precluded Mr. Boyce's employment, but might have precluded his being cleared.

Q: In hindsight, do you believe it was a wise management decision to place a young, unproven and untested individual like Christopher Boyce into a position at the heart of your most sensitive operations? Dr. Flyer suggested yesterday that we should be "selecting people into high risk positions, rather than screening them out." Don't you think that advice is appropriate in light of the Boyce case?

A: There is no statistical evidence which supports the thought that a young, unproven individual is less likely to be trustworthy. We are not sure, under the clearance procedures in effect at that time, that, even following Dr. Flyer's suggestion, Mr. Boyce would not have been selected. However, we have no quarrel with the philosophy of "selecting in."

In light of the Boyce case, TRW has elected to put entry level security personnel into less sensitive jobs for a period of 12-18 months so that we have a period of time in which to make a personal assessment of the individual's suitability for more sensitive positions.

Q: As a result of the Boyce case, it is our understanding that Mr. Carr prepared an internal memorandum making certain recommendations for improved security. Would you please provide the Subcommittee with that memo? What were those recommendations? Have you carried them out?

A: Following the Boyce case, Mr. Carr provided a wide-ranging list of suggested security improvements for review by management and by the Government. Those recommendations, as submitted to management, are attached.

The majority of the recommendations -- many of which exceeded government requirements -- were implemented. Those requiring Government participation were proposed to the Government.

Detailed information on security measures adopted by industry and by Government as well as procedures not required by Government which were implemented at TRW are provided in our written statement.

Q. Do you feel that present government policy should be changed to permit the granting or continued holding of a security clearance to be a condition of employment?

A. We could support such a policy change and suggest that, if it is appropriate for industry, it might also be appropriate for Government. For large organizations such as TRW, with a diverse range of sensitive and non-sensitive jobs, such a policy change would not be a major issue. However, for smaller organizations, making a security clearance be a condition of employment could help them terminate employees they would otherwise have to carry in non-productive positions.

Q: Do you feel that contractor security personnel should have access to the privacy portions of clearance applications?

A: Employers are prohibited by various federal and state statutes as well as judicial and administrative interpretations from soliciting certain kinds of information from applicants or employees. The issue may not so much be access to privacy portions of clearance applications as much as removing barriers during the hiring process to contractors having such information as arrest records, foreign origins, and substance abuse problems. In addition, we suggest that removing the barrier to pre-employment clearances, currently part of the Industrial Security Manual, would also address the real issue presented in your question. We believe that the responsibility of clearing personnel or denying clearances should remain with the Government.

Q: The DOD report found that "DOD mandated and contractor initiated physical and personnel security controls during non-working hours, to the extent they exist, are generally weak and ineffective, and, as such, provide inadequate protection against unauthorized access or removal of classified material."

Should DOD required security controls be enhanced during non-working hours at cleared Defense contractors authorized to store classified material on the premises?

A: At TRW, there are several components to after-hours security: Use of coding on each employee's special access badge along with a digital code entered by the employee identifies employee access authorization and records the time and date of each entry. Thus, there is a record which supervisors and security officers can check. This system supplements the primary access control, which is face-to-face identification by security officers. We have adopted a policy of random search, with signs posted at exits. We use television monitors in sensitive and non-sensitive areas. In areas where the two-man rule is applied, it is applied 24 hours a day. We also randomly rotate security people. And, among our document control procedures, we have adopted the use of the magnetic metallic strips for certain sensitive documents, with alarm systems at exits.

It is company policy that all classified documents be secured in a safe container and never left unattended. Roving security officers police every building to check on after-hours occupants and to assure that all containers and vaults are secured.

We believe that these procedures constitute an effective deterrent and significantly improve after-hours security.

We should point out that Mr. Boyce was wrong in his assessment of the two-man rule. Our procedures, combined with computerized access systems, effectively prevent a single person from being in an area where two people are required, regardless of the reason.

Q: In each of the three cases which you are familiar with, the William Holden Bell case at Hughes, the Harper-Schuler case at SCT, and the Christopher Boyce case at TRW, extensive classified information was lost. Yet in none of them were the contractors themselves held accountable in any way for the breaches in security. It was as if the contractors were seen as mere spectators to espionage with little responsibility for what happened. No fines were levied, no disciplinary action was taken, no contracts were lost. Critics of the current system say that is wrong, that contractors should be held accountable for security failures. If the contractors were held accountable to some extent for the conduct of their employees, might that not result in increased security in the defense industries?

A: We do not agree with the critics that a general blanket policy of punitive action is appropriate. However, we believe that, as in the Boyce case, a comprehensive investigation by the Government should take place and appropriate action be taken based on the findings. The DISP currently provides for actions to be taken against a contractor where warranted.

There has never been any lack of incentive on TRW's part to run a top-notch security program that protects the vital security interests of our nation. We share that incentive with our government counterparts. We would also suggest that, while we can learn from these tragedies, we must remember that Christopher Boyce committed his crime nearly ten years ago. Since then, all of us -- industry and government alike -- have refined and improved our procedures and applied new technology.

Each situation must be reviewed in detail, as it was in the Boyce case. Despite a limited number of problems, the fact is TRW was complying with security regulations then in effect, and the Government's own investigation -- one of the most comprehensive conducted at that time -- did not find TRW guilty of wrongdoing warranting disciplinary action.

In looking at the question of punitive action, it is important to remember that no security system is invulnerable. Everyone involved with security must be aware of the vital element of human integrity.

Q. In your opinion, what is the biggest problem with our current personnel security program?

A. People, who are an essential component of our national security program, are also the weakest link. In the selection of personnel, there is no foolproof system of testing for integrity and other qualities of character that make for a loyal citizen. There is also no known way of identifying what is happening in an individual's life that may change his or her stability.

Assuring that only the most trustworthy and qualified people are "selected in" to sensitive programs would require a review of the quality control procedures associated with background investigations. Enhancement of the investigative process, which is already backlogged, would also have budget and staffing implications for the Government.

Q. Do security protection standards for the handling of classified material vary between government and industry? If so, does this pose a problem to industry?

A. There are different standards between government and industry, but we do not view this as a problem.

Q. Should DIS establish a nationwide security hotline for receipt of anonymous information (6(b)(1) of the Industrial Security Manual) impacting on the Defense Industrial Security Program?

A. TRW does not believe a hotline is warranted. Like many hotline systems, it could be subject to abuses because of the very personal nature of the information involved. The appropriate place for such issues to be raised is within the workplace, through the normal management channels for such issues. TRW encourages its employees to raise problems to our Security Department or, if they are uncomfortable with that, to contact the FBI.

Q. Should the inspection rating system be changed from satisfactory/unsatisfactory to a graded system such as outstanding, superior, satisfactory, marginal, and unsatisfactory?

A. No, we do not believe the addition of several categories of performance would add anything to the protection of the nation's classified assets, although the expansion of the security incentives programs for good performance could be useful (see next question).

Q. In many "carve out" or "black" contracts, an award provision for security is utilized. What are your feelings about such a proposal for Secret and particularly sensitive DOD contracts?

A. As we mentioned in testimony, we believe that security incentive clauses bring added value in terms of management attention, and should be considered on a selective basis in non-SCI contracts. We have found them to be an effective tool in reminding management of security requirements and of the constant need for a complete security program.

Q. Should fulltime DIS representatives be assigned to contractor facilities, as recommended by the DOD Harper Report?

A. No. Close working relationships as well as the proximity of major DIS field offices to large contractors are sufficient. We cannot speak for smaller contractors.

Q. What could have been done to have either prevented or deterred Christopher Boyce?

A. Recognizing that Mr. Boyce committed his crimes nearly a decade ago, we will respond to what systems in use or contemplated today might have made a difference.

We have previously discussed the enhancements to background investigations -- including emphasis on peer relationships -- which might have raised "red flags" in Mr. Boyce's case. We also discussed TRW's procedure for placing entry level personnel into non-sensitive positions for further evaluation prior to placing them in sensitive positions.

If Mr. Boyce were cleared today, he would confront numerous controls which might have deterred him. These are described in our written statement and oral testimony; they include: random searches, the use of Government-administered polygraph examinations of those individuals in highly sensitive positions, the use of magnetic metallic strips on certain sensitive documents, and the two-person rule in certain sensitive areas.

While we acknowledge that there were a small number of security problems at TRW, neither Mr. Boyce, the Government agency which investigated the situation, TRW which conducted its own self-analysis, nor the Federal court before which Mr. Boyce was tried and convicted was able to substantiate much of what Mr. Boyce alleged at his trial and before this Subcommittee. In fact, Judge Robert Kelleher, who heard several weeks of testimony by Mr. Boyce, said, "The Court didn't find any veracity in him ... The Court didn't believe a word the defendant expressed on any material issue."

Our nation's security system in the final analysis depends on people. The case of Christopher Boyce demonstrates that it is individuals who become traitors, not systems or procedures.

Q. Do you have any recommendations for legislative action which would enhance personnel security?

A. We would recommend a review of existing Federal and state legal and regulatory prohibitions which make the hiring and clearance processes more difficult for contractors and Government alike. For example, state laws providing for the sealing or expunging of certain criminal -- including juvenile -- records hamper the Government investigative process. Access by individuals to their security investigation file under FOIA limits the Government's ability to provide confidentiality to interviewees. For contractors, EEO guidelines prohibit inquiries on foreign origins or relationships, and contractors are restricted from obtaining information on arrest records and sealed and expunged conviction records. In many states there are restrictive laws on polygraph testing.

Q. Would you furnish a copy of your internal investigation of the Boyce espionage case, as promised during your testimony?

A. There is no written record of our internal self-analysis except for the recommendations, which were made to management and to the Government in 1977, referenced in our response to an earlier question and attached. Our emphasis was on developing thoughtful recommendations which would deter problems and further enhance security procedures.

Q. Would you furnish a copy of any records indicating the time lag in your requests for clearances and how that delay relates to your company's productivity, as promised during your testimony?

A. The primary costs of delays in processing clearances are those associated with program costs when an employee assigned to a program cannot work on his or her assignment due to lack of a clearance. In addition to the dollar estimates of program delays is the potential impact of these delays on our nation's security.

TRW has not conducted its own studies on the cost impact of such delays in clearance processing. We would, however, respectfully direct your attention to the Comptroller General's Report to the Congress of the United States, titled, "Faster Processing of DOD Personnel Security Clearances Could Avoid Millions in Losses," dated September 15, 1981.

Q. Would you furnish a copy of the number of 6(b) violations reported by your company for the last five (5) years?

A. Under provisions of paragraph 6(b)(1), requiring the reporting of adverse information which could affect an individual's ability to protect classified information, TRW made 118 reports during 1984, 18 in 1983, 18 in 1982, 15 in 1981, and 28 in 1980. As we pointed out in response to a Subcommittee question on this subject, the Defense Investigative Service in 1985 complimented TRW for its particularly aggressive program in reporting such adverse information.

Q. You indicated in your testimony that within a significant fraction of your special compartmentalized special projects, you have some clauses for security built into the contract provisions. Were such provisions included into the contract or contracts which Boyce was convicted of espionage? If so, did you receive monetary amounts for your security performance?

A. There were security provisions in the contract in question. There were no incentive fee awards for security on the contract for which Mr. Boyce was convicted of espionage. Post Boyce, a security incentive program was adopted by the Government agency involved. Today, only certain SCI customers and "carve out" programs offer such security performance incentives. We have, since their inception, received numerous incentive fees for the quality of our security procedures.

Q. During the time frame of Boyce's espionage, did you receive any security awards, whether monetary or otherwise, from any government agency? If so, list by agency, award and amount.

A. TRW received the Cogswell Award from the Defense Supply Agency in 1975 for sustained, outstanding performance on the Defense Industrial Security Program in 1974. No monetary award is associated with this recognition.

Corrective Action by TRW Security

The following guidelines and changes of systems are recommended for implementation at TRW to aid in the prevention of any future compromise. TRW security will engage in discussions of these guidelines and systems with the customer for their approval prior to industrial wide implementation. In these discussions, the customer will be apprised of the possible impedence to invoking changes because of United States and State laws and regulations. The customer security groups must act either by executive order publication or change in present laws to permit imposition of more strenuous regulations for the "interest of national security".

1. Identify those sensitive areas wherein there will be a policy, that no one is ever to be engaged in work alone. Communications, Graphics, Security, Study Tanks.
    a. Areas of documentation or hardware that will be opened and closed by two people and never be unattended. (To be implemented).
    b. Double keying of areas — two man rule. (To be implemented).
    c. Television monitoring can be inplanted, both night and day, of personnel activities. (To be implemented).
    d. Further introduction of the Secure Access Control Systems (SACS), for all sensitive areas to allow computerized registry of persons entering and exiting these areas. Monitoring of the computer records of those people entering the area on off-duty and weekend hours. (To be implemented).
    e. Possible recommendations of delayed frame cameras to be installed for after duty hours in super sensitive areas. (No implementation).
2. Make it a job requirement for personnel assignment in certain areas, personnel will be advised condition of assignment is based upon:
    a. A periodic interview by management as to personal activities.
    b. Waiver of privacy will be requested. (To be implemented).
    c. Have a credit check and an inquiry as to financial matters. (To be implemented.).
    d. After a discussion with DSSG legal, a possibility of polygraph testing. (Implementation at TRW).
    e. A periodic background check will be conducted by TRW investigative group.
    f. Monitoring of Company records for utilization of time off sick, vacation, leave. (To be implemented).

3. Forbid any introduction or removal of packages, parcels, envelopes from the sensitive areas, without double coverage of delivery. There will be physical posting of Company's right to examine at each entrance and exit to all sensitive areas. (To be implemented).

    a. All packages, envelopes, briefcases subject to examination upon entrance and exit in sensitive areas. (To be implemented).

    b. Install magnetometer entrance control. (Not recommended).

4. Rigid adherence of the filing of foreign travel which will include, in depth, identification of time, place and purpose of visit for all foreign travel. Debriefing on return. (To be implemented).

5. A semi annual reindoctrination and affirmation of security oath for all personnel assigned to sensitive areas. Reading of espionage laws will be required and the booklets will be issued to each person. (To be implemented).

6. Special security will pursue the possibility of any device that could be impregnated into document forms or format which could be detected on removal from an area. (To be implemented). Example: 3M library sensor system.

7. Random security inspections are required and discussions will be conducted with the customers as to this activity. (To be implemented).

    o Customer and Contractor internal

        Document Control

        Container Inspections

        Badge Control

        Lock & Key Accountability (Rigid)

        Access Control

        Security Awareness Interviews

        Non Duty Hour Inspections

8. Reproduction machines will be controlled and equipped with counters. (To be implemented).

9. A total review as to proper staffing will be conducted, looking toward maturity of personnel and compensation commensurate to the responsibilities of the job function. (To be implemented).

10. An annual rotation of personnel to preclude incestuous relationships from developing. (To be implemented).

11. A program of training for the security officers for special areas will be imposed. The major purpose of this will be to motivate the security officer force as to their responsibility and the reason for the areas being designated as sensitive. (To be implemented).

12. All personnel History Statements of employees 30 years of age and under will be required to list 5 names of associates of peer groups for interview as to possible suitability. (Customer Action).

13. Embark on a positive education program to break down the code of silence which exists among most peer working groups for report of possible misconduct. Furnish to the employees working in sensitive areas the need for complete openess and how misconduct impacts the security obligations for the security sensitive areas. (To be implemented).

14. In communications areas, wherein cipher key decks are utilized, daily issuing of the card for commo set will be issued and the setting of the machine will be accomplished by 2 individuals. There will be no breaking of the card deck, except for one day issuance. (Customer Action).

15. Inadvertent spill of communication messages will be recorded and examined by the supervisor at both the receiver and senders locations, and the receiver will forward to the sender the original copy for verification of destruction, log and record. (Customer Action).

16. Publish guidelines as to information transfer within the rigid compartmentation. (Customer Action).

17. No open shelf storage in communications rooms. Accountability of container for compartmented security. One project per container — no mixing therein of various projects. (Customer Action).

18. Consolidate TWX functions into common area for more effective protection of material. Recommend customer staffing of this area. (Customer Action).

19. Rebadging of all personnel assigned to all restricted areas to establish again the positive need-to-know. (To be implemented).

Statement of Richard M. Welby
Assistant Director, Corporate Security
Hughes Aircraft Company

Mr. Chairman and Members of the Permanent Subcommittee. My name is Richard M. Welby, Assistant Director, Corporate Security, Hughes Aircraft Company. I am here at the invitation of this Subcommittee to testify on behalf of the Hughes Aircraft Company, El Segundo, California.

I would like to give you a brief description of the Hughes Aircraft Company's security program, our comments on some of the recommendations of the Department of Defense Industrial Security Review Committee and status of our company's security program before and after the William H. Bell case.

Hughes Aircraft Company has capabilities in advanced electronics, space and communications, missiles and avionics, air defense, command and control, industrial electronics, and basic research. Its activities span more than 1,500 projects and include over 12,000 separate products, services, and functions.

Hughes employs approximately 74,000 employees - including over 23,000 on the scientific and engineering technical staff who work in fully-equipped facilities encompassing more than 19 million square feet of floor space. The company is made up of seven major product organizations.

There are sixty cleared company facilities with established Security Practices and Procedures outlining the requirements of the Defense Industrial Security Program. Approximately 1,035 security personnel are directly assigned to administer and implement the company security program for meeting the requirements of the Defense Industrial Security Program.

Company security organizations are responsible for administering programs for:

> Personnel Security which involves the processing of personnel and facility security clearances, visitor clearances, and investigations.
>
> Physical Security which assures protection of company facilities, classified material access controls, identification systems and visitor control. Most of Hughes facilities maintain twenty-four hour guard coverage of their locations.
>
> Information Security which assures the proper handling, marking, transmittal, destruction, accountability, etc. of all classified material.

Company facilities are cleared by the government at the Top Secret and Secret level with equivalent storage capabilities which qualifies the company to bid, receive, and perform on contracts requiring access to classified material at these levels.

Approximately ninety percent of all Hughes 74,000 employees are cleared as follows:

Top Secret:	2,000
Secret:	35,000
Confidential:	26,000
Uncleared:	11,000

Defense Investigative Service Cognizant Security Offices inspect all areas of the company's implementation of the Defense Industrial Security Program on a biannual basis. Periodical inspections are also conducted of the company's Arms, Ammunition, and Explosives (AA&E) Program, Industrial Facilities Protection Program (IFPP), and Operations Security Program (OPSEC).

The company conducts biannual self-inspection of the Government Security Program and an annual inventory of all Top Secret and Secret material. In addition, employees are issued statements of their Secret document holdings every three months. Currently 2,300 employees have Secret documents in their custody.

Following is the approximate number of classified documents at Hughes Aircraft Company.

50 Top Secret documents
100,000 Secret documents
800,000 Confidential documents
120 Closed Areas containing classified hardware
70 computer systems which process classified information

The company is currently performing on approximately 1,200 prime contracts and subcontracts with U. S. Government User Agencies and other major contractors which require access to classified information.

The company issues over 1,400 purchase orders to subcontractors each year involving procurement of classified parts and services in support of prime and subcontracts.

In support of these contracts, company security organizations process approximately 10,000 incoming visits and 18,000 outgoing visits annually.

Company security organizations are responsible for conducting investigations of administrative security infractions/violations, thefts, sabotage, violations of company rules, etc.

The Company has an ongoing security education and training program which is mainly directed toward the requirements of the Industrial Security Manual for Safeguarding Classified Material. It consists of new employee security orientation and briefings, scheduled classes on the handling of classified material, special indoctrination and training sessions on new Industrial Security Manual requirements, foreign travel briefing, briefings on the handcarrying of classified material, and foreign intelligence briefings.

The following represents a brief summary of comments concerning the Defense Industrial Security Review Committee recommendations.

Of the 38 responses requested in the 25 recommendations, we concurred with 15, disagree with 18, and have no comment comment on 5 of the items.

The Committee's recommendations with which we are primarily concerned include:

#3. We disagree with the replacement of the ISM but do feel it should be reorganized.

#4. We strongly concur with the DIS inspection of Special Access Programs.

#8. We strongly disagree with reporting all foreign travel in that it would be too costly and would serve no useful security purpose.

#10. We see no need for a "National Industrial Security Hotline" on the basis of additional costs, plus most allegations would be inconclusive and unproductive.

#19. In regard to the recommendations concerning the enhancement of Personnel Security Investigative Standards and Reduction of Industrial Clearances, we concur with items 19a, b, c, e, and f, but feel items 19d, g, h, i, and j would either be too costly or serve no useful security purpose.

#24. We totally agree with the recommendation for the increased emphasis on classification management. We feel classification management is one of the more important parts of DISP in that it identifies that information and material requiring protection in the interest of national defense. We also feel that major changes are required concerning the length of time material remains classified.

William H. Bell Incident

The company's investigation of the William H. Bell case indicated that the incident did not result from a weakness in our security program or classified document accountability system, but from willful security violations by a longtime employee.

Our investigations revealed that William Bell intentionally violated company and government security regulations by illegally removing classified documents from company premises. There is just no way to prevent such unauthorized removals short of conducting a physical search of each employee as he/she departs company premises.

Our investigation of the incident revealed that the Secret documents charged to Bell were properly accounted for and surrendered by him at the time of his termination.

Concerning Bell's possession of multiple copies of classified documents, this is not an uncommon practice for program managers. Bell, being a program manager, was authorized to request additional copies from Document Control.

Annually, the Company conducts a Secret document inventory of all custodians, at which time they are required to justify retention of Secret documents in their possession. In addition, employees are requested to reduce the number of classified documents, and inspections are frequently conducted with the intent of reducing the number of classified documents in the employees' possession.

By Company Bulletin, 29 June 1981, to all Hughes Aircraft Company employees Dr. Puckett expressed his concern for the Bell incident. He reminded us of the sensitive nature of our work and the absolute necessity of adhering to company security practices.

We believe our security and classified document accountability systems function efficiently and effectively; however, the best system still depends upon the integrity of the individual.

Volume I - Part I and Part II

SUMMARY OF THE HUGHES AIRCRAFT COMPANY SECURITY PROGRAM

February 1985

Hughes Aircraft Company has capabilities in advanced electronics, space and communications, missiles and avionics, air defense, command and control, industrial electronics, and basic research. Its activities span more than 1500 projects and include over 12,000 separate products, services, and functions.

Hughes employs approximately 74,000 employees - including over 23,000 on the scientific and engineering technical staff who work in fully equipped facilities encompassing more than 19 million square feet of floor space. The company is made up of seven major product organizations plus a research laboratory.

HUGHES SECURITY POLICY/PRACTICES/PROCEDURES

Hughes top management is vigorous in its support of the company security program for the implementation of the Defense Industrial Security Program.

The Corporate Office and each of the fifty-nine cleared company facilities have in force Security Practices and Procedures outlining the requirements of the Defense Industrial Security Program. Approximately 1035 security personnel are directly assigned to administer and implement the company security program for meeting the requirements of the Defense Industrial Security Program.

FUNCTIONS OF HUGHES SECURITY ORGANIZATIONS

Company security organizations administer the programs for personnel, physical, information and special programs security.

Personnel security involves the processing of personal and facility security clearances, visitor clearances, and investigations.

Physical security assures protection of company facilities, classified material access controls, identification systems and visitor control. Most of Hughes facilities maintain twenty-four hour guard coverage of their locations.

Information Security deals with the handling, marking, transmittal, destruction, accountability, etc. of all classified material.

FACILITY SECURITY CLEARANCES

Company facilities are cleared at the Top Secret and Secret level with equivalent storage capabilities. The Facility Security Clearances qualify the company and its facilities to bid, receive, and perform on contracts requiring access to classified material to the levels of Top Secret and Secret.

Approximately ninety percent of all Hughes 74,000 employees are cleared as follows:

Top Secret: 2,000
Secret: 35,000
Confidential: 26,000
Uncleared: 11,000

In addition, 2,648 employees have been briefed for access to NATO, CNWDI, and COMSEC classified material as follows:

1,010	North American Treaty Organization (NATO)
959	Critical Nuclear Weapon Design Information (CNWDI)
679	Communication Security (COMSEC)

SECURITY INSPECTIONS

Defense Investigative Services Cognizant Security Offices inspect all areas of the company's implementation of the Defense Industrial Security Program on a biannual basis. Inspections are periodically conducted in the handling of the Arms Ammunition, and Explosives (AA&E) Program, the Industrial Facilities Protection Program (IFPP), and the Operations Security Program (OPSEC).

The company conducts biannual self-inspection of the Government Security Program and conducts an annual inventory of all Top Secret and Secret material.

CLASSIFIED MATERIAL

The company and its cleared locations maintain systems for the accountability and protection of all classified material as follows:

50 Top Secret Documents
100,000 Secret Documents
800,000 Confidential Documents
120 Closed Areas containing classified hardware
70 computer systems which process classified information

CLASSIFIED CONTRACTS (PRIME AND SUBCONTRACTS)

The company is currently performing on approximately 1200 prime contracts and subcontracts with U. S. Government User Agencies and other major contractors which require access to classified information.

CLASSIFIED SUBCONTRACTING

The company issues over 1400 purchase orders to subcontractors each year involving procurement of classified parts and services in support of prime and subcontracts.

VISIT CLEARANCES

Approximately 10,000 incoming visits are processed on an annual basis.

Approximately 18,000 outgoing visits are processed on an annual basis.

INVESTIGATIONS

Company security organization investigators and inspectors conduct:

Investigations of administrative security infractions/violations.

Investigations into thefts, sabotage, violation of company rules, etc.

Investigations of lost classified documents and preparation and submittal of the required reports to DIS Cognizant Security Office of possible or suspected compromise.

SECURITY EDUCATION AND TRAINING

Hughes Aircraft Company's security education and training program is mainly directed toward the requirements of the Industrial Security Manual for Safeguarding Classified Material. It consists of new employee security orientation and briefings, scheduled classes on the handling of classified material, special indoctrination and training sessions on new Industrial Security Manual requirements (i.e., new Executive Order marking requirements), security representative meetings, foreign travel briefing, and briefings for handcarrying classified material.

Volume I, Part I

DETAILS OF THE HUGHES AIRCRAFT COMPANY SECURITY PROGRAM FOR IMPLEMENTATION OF THE DEFENSE INDUSTRIAL SECURITY PROGRAM

February 1985

Hughes Aircraft Company specializes in high-technology electronics, continually advancing in this field until today its products are in use throughout many sectors of the scientific, commercial and military communities.

Company activities span more than 1500 projects and include over 12,000 separate products, services, and functions - ranging from basic research and engineering to quality manufacturing and field support.

The company has capabilities in advanced electronics, in space and communications, missiles and avionics, air defense, command and control, industrial electronics, and basic research.

Hughes employs approximately 74,000 employees - including over 23,000 on the scientific and engineering technical staff who work in fully equipped facilities encompassing more than 19 million square feet of floor space. Extensive facility construction is under way to keep pace with company developments.

Hughes Aircraft Company is organized on a decentralized basis to allow each major group to concentrate its efforts on a specific area within the electronics industry - each with a total capability from research through sales.

The company is made up of seven major product organizations: Electro-Optical and Data Systems Group, Ground Systems Group, Industrial Electronics Group, Missile Systems Group, Radar Systems Group, Space and Communications Group, and Support Systems. In addition there are the company's Research Laboratories, which operate in both basic and product-directed research programs of scientific significance to the company.

HUGHES SECURITY POLICY/PRACTICES/PROCEDURES

Top management support of the Hughes security program in implementation of the Defense Industrial Security Program is contained in Company Policy Number 11-1 (revised) dated 10/18/78. Dr. Allen E. Puckett issued the policy when he was President of the company.

Eighteen Corporate Security Practices (Attachment II) are in force addressing the company's overall security program for implementation of the requirements of the Defense Industrial Security Program for safeguarding DoD classified and sensitive company information and material.

In addition, each of the fifty-nine cleared company facilities/locations maintain a set of Security Practices and Procedures outlining the requirements of the Defense Industrial Security Program. Attachment III is one example of these Security Practices and Procedures.

HUGHES SECURITY ORGANIZATIONS

The attached charts (Attachments IV and V) outline the security organizations of the corporate office and other cleared company locations. On a whole, approximately 1,035 security personnel are directly assigned to administer and implement the company security program for meeting the requirements of the Defense Industrial Security Program.

FUNCTIONS OF HUGHES SECURITY ORGANIZATIONS

CORPORATE SECURITY

Maintains and administers the Department of Defense Top Secret Facility Clearance for the home office in El Segundo

Establishes policies and practices for company-wide implementation of the following security functions.

Personnel/Physical Security

- Personnel and Facility Security Clearances
- Visitor Control/Clearances
- Plant Protection (gate, lobby and perimeter control)
- Fire Protection
- Industrial Defense/Emergency Planning/AA&E Program
- Lock and Key Control
- Investigations
- Identification Systems (employee/visitors)
- Executive Protection

Information Security

- Classification Management
- Procedures for Marking and Handling of Classified Material
- Government Security Inspections
- Security Education and Training

Disciplinary Program for Security Violations
Master Document Control and Accountability
Automatic Data Processing Security
Retention/Disposition of Classified Material
Security Self-Inspections

CLEARED COMPANY LOCATIONS SECURITY

Security personnel at all cleared company locations establish security operating practices and procedures based on the aforementioned Company Policies and Practices and administer the company's program for implementation of the requirements of the Defense Industrial Security Program at their respective locations.

FACILITY SECURITY CLEARANCES

The Department of Defense and Hughes Aircraft Company cleared facilities jointly executed Department of Defense Security Agreements (DD Form 441) for Top Secret and Secret facility security clearances with equivalent storage capabilities. These agreements call for the Company:

To provide and maintain a system of security controls in accordance with the Industrial Security Manual for Safeguarding Classified Material (DoD 5220.22-M).

To permit periodic security inspections by the Defense Investigative Service Cognizant Security Offices.

To submit to the Government a Certificate Pertaining to Foreign Interests (DD 441s) which is a complete report concerning the company's Foreign Ownership Control and Influence (FOCI) and any arrangements with foreign governments to include an account of total income, foreign affiliations, etc.

To submit a report of any changes to the Owners, Officers, Directors, and Executive Personnel (OODEPs) of the company and a statement concerning any foreign representation/interest.

ACCESS TO CLASSIFIED DEFENSE INFORMATION

The Facility Security Clearances qualify the company and its facilities to bid, receive, and perform on contracts requiring access to classified material to the levels of Top Secret and Secret.

All employees requiring access to Top Secret or Secret information are cleared by the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio.

Employees requiring access to Confidential material are granted Confidential clearance by the facility security office at each cleared company location.

Due to the nature of our business, approximately ninety percent of all Hughes 74,000 employees are cleared as follows:

Top Secret: 2,000
Secret: 35,000
Confidential: 26,000
Uncleared: 11,000

Special briefings are required for access to NATO, CNWDI, and COMSEC classified information - 2648 employees have been briefed as follows:

1,010: North Atlantic Treaty Organization (NATO)
959: Critical Nuclear Weapon Design Information (CNWDI)
679: Communications Security (COMSEC)

SECURITY INSPECTIONS

Defense Investigative Services Cognizant Security Offices

Inspect all areas of the company's implementation of the Defense Industrial Security Program on a biannual basis.

Annually inspect the handling of the Arms, Ammunition, and Explosives (AA&E) Program and the Industrial Facilities Protection Program (IFPP).

Conduct inspections concerning the Operations Security Program (OPSEC).

Other Government Agency Inspections

AFPRO Fire Protection
Government Industrial Defense Organizations

COMSEC/CRYPTO (NSA and U.S. Air Force)
Individual DoD User Agencies

Company

Biannual Self-Inspection of Government Security Program (required by the ISM)
Periodic Inspection of Procedures for Protection of Company Sensitive Information
Fire Protection/Prevention
Secret Document Accountability Inventory (annual)

CLASSIFIED MATERIAL

The company and its cleared locations maintain systems for the accountability and protection of all classified material.

All DoD Top Secret Documents - Approximately 50
Currently accounts for over 100,000 Secret Documents
Maintains protection of over 800,000 Confidential Documents
Protects Classified Hardware in 120 Closed Areas
Maintains over 70 computer systems which process classified information

CLASSIFIED CONTRACTS (PRIME AND SUBCONTRACTS)

The company is currently performing on prime contracts and subcontracts with U.S. Government User Agencies and other major contractors which require access to classified information.

The company is currently performing on over 1200 classified contracts.

For each classified contract a Contract Security Classification Specification (DD Form 254) is received from the Government User Agency which provides security classification guidance to be applied to information generated.

Copies of the DD 254 are sent to DIS, the company's Cognizant Security Office. This enables the Cognizant Office to monitor the protection of material pertaining to each contract.

CLASSIFIED SUBCONTRACTING

The company issues over 1400 purchase orders to subcontractors each year involving procurement of classified parts and services in support of prime and subcontracts.

A DD254 is prepared for each purchase order by a member of the concerned company security office and approved by the responsible ACO or contracting officer of the prime or subcontract.

The Facility Security Clearance of each subcontractor is also verified by the company security office through the subcontractor's Cognizant Security Office.

SECURITY CLEARANCES

In support of the company's performance on classified contracts the following security clearance actions are required to be taken by company security organizations.

Personnel Security Clearances/Briefings

DD Forms 48, 48-3, and 49 are processed to the Defense Industrial Security Clearance Office (DISCO) for all employees requiring Secret or Top Secret clearances.

DD Form 48-2s are completed by employees requiring access to Confidential information. Confidential clearances are granted by the Company's Security Officer upon satisfactory completion of the form and verification of the employee's U.S. citizenship.

All new employees receive, upon hire, an in-depth security briefing and orientation.

Visitor Clearances

Incoming Visits - Facility and personnel security clearances of visitors to Hughes are processed for verification and approval. Those not directly related to a specific contract require ACO approval. Approximately 10,000 incoming visits are processed annually.

Outgoing Visits - Visit Request and Authorization forms are processed, approved, and forwarded to the DoD User Agency and contractors verifying company employees' security clearance and need-to-know prior to all visits. Approximately 18,000 outgoing visits are processed annually.

INVESTIGATIONS

Company security organization investigators and inspectors conduct:

Investigations of administrative security infractions/violations.

Investigation into thefts, sabotage, violation of Company rules, etc.

Investigations of lost classified documents and preparation and submittal of the required reports to DIS Cognizant Security Office of possible or suspected compromise.

Pre-employment screening of applicants for hire.

Post-employment verifications of new employees' prior employment, education, etc.

SECURITY EDUCATION AND TRAINING

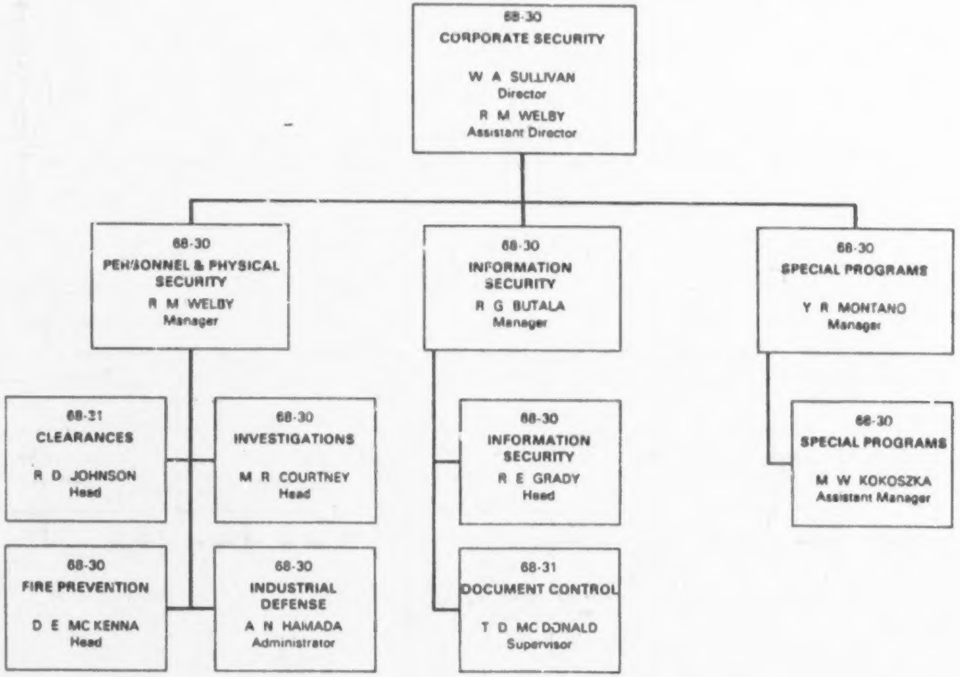
Hughes Aircraft Company's security education and training program is mainly directed toward the requirements of the Industrial Security Manual for Safeguarding Classified Material. It consists of new employee security orientation and briefings, scheduled classes on the handling of classified material, special indoctrination and training sessions on new Industrial Security Manual requirements (i.e., new Executive Order marking requirements), security representative meetings, foreign travel briefing, and briefings for handcarrying classified material. A booklet entitled You and Hughes Security is given to each new employee during new employee indoctrination sessions. A publication entitled Classified Material Handling Guide is issued to employees who attend scheduled training sessions. These sessions are designed for employees who handle and generate classified material on a regular basis.

The education and training program includes a security poster program whereby approximately six posters per year are prepared in-house and posted throughout the company. Articles are also published in the company newspaper concerning current security items of interest and concern to all employees. A periodic publication entitled Security Views is distributed to each employee, highlighting new or changed security requirements as well as items of concern identified during self inspections and "696" cognizant security office inspections. Security organizations of individually-cleared company facilities also prepare and distribute security bulletins identifying security items of concern and interest. DISI's Security Awareness Bulletin is distributed to all company locations for their information and use.

Attachment VI contains copies of the above-mentioned items as well as other educational material used throughout the company.

COMPANY ORGANIZATION MANUAL
HUGHES AIRCRAFT COMPANY

HUMAN RESOURCES & ADMINISTRATION


68-30
CORPORATE SECURITY
W A SULLIVAN
Director
R M WELBY
Assistant Director
68-30
PERSONNEL & PHYSICAL SECURITY
R M WELBY
Manager
68-30
INFORMATION SECURITY
R G BUTALA
Manager
68-30
SPECIAL PROGRAMS
Y R MONTANO
Manager
68-31
CLEARANCES
R D JOHNSON
Head
68-30
INVESTIGATIONS
M R COURTNEY
Head
68-30
FIRE PREVENTION
D E MC KENNA
Head
68-30
INDUSTRIAL DEFENSE
A N HAMADA
Administrator
68-30
INFORMATION SECURITY
R E GRADY
Head
68-31
DOCUMENT CONTROL
T D MC DONALD
Supervisor
68-30
SPECIAL PROGRAMS
M W KOKOSZKA
Assistant Manager

Approved W A Sullivan
Director,
Corporate Security

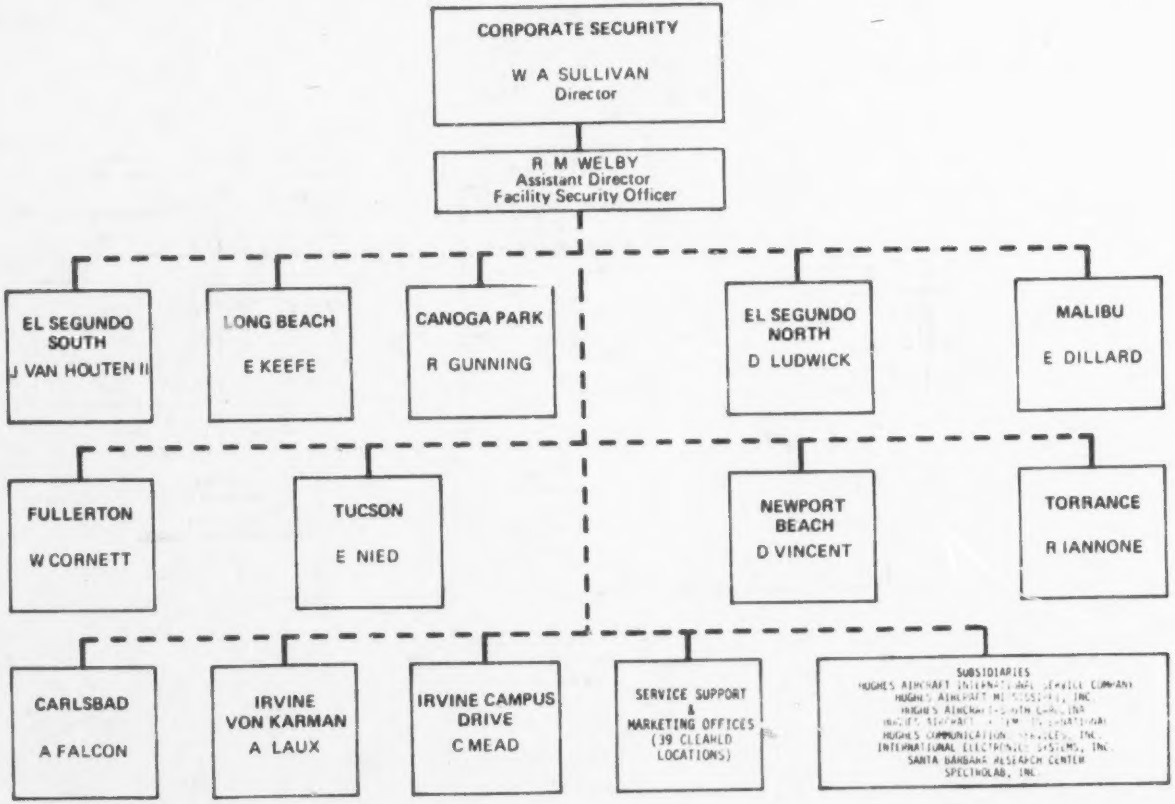
NEW CHART — FIRST ISSUE

Date 5-12-83

Chart 68-30

HUGHES AIRCRAFT COMPANY

FACILITY SECURITY ORGANIZATION


CORPORATE SECURITY
W A SULLIVAN
Director
R M WELBY
Assistant Director
Facility Security Officer
EL SEGUNDO SOUTH
J VAN HOUTEN II
LONG BEACH
E KEEFE
CANOGA PARK
R GUNNING
EL SEGUNDO NORTH
D LUDWICK
MALIBU
E DILLARD
FULLERTON
W CORNETT
TUCSON
E NIED
NEWPORT BEACH
D VINCENT
TORRANCE
R IANNONE
CARLSBAD
A FALCON
IRVINE VON KARMAN
A LAUX
IRVINE CAMPUS DRIVE
C MEAD
SERVICE SUPPORT & MARKETING OFFICES (39 CLEARED LOCATIONS)
SUBSIDIARIES
HUGHES AIRCRAFT INTERNATIONAL SERVICE COMPANY
HUGHES AIRCRAFT MISSISSIPPI, INC.
HUGHES AIRCRAFT-SOUTH CAROLINA
HUGHES AIRCRAFT SYSTEMS INTERNATIONAL
HUGHES COMMUNICATION SERVICES, INC.
INTERNATIONAL ELECTRONIC SYSTEMS, INC.
SANTA BARBARA RESEARCH CENTER
SPECTROLAB, INC.

February 1985

Volume II

COMMENTS OF HUGHES AIRCRAFT COMPANY ON RECOMMENDATIONS OF THE DoD INDUSTRIAL SECURITY REVIEW COMMITTEE

Following are Hughes Aircraft Company's comments concerning the recommendations for changes in the Defense Industrial Security Program.

1. Increased Emphasis on Counterintelligence and Human Reliability Within the Defense Industrial Security Program (DISP)

COMMENT:

We concur with the concept of a threat awareness program; however, if implemented, government rules and regulations concerning release of intelligence information to contractors would require revision. Also, in order for contractors to be proactive instead of reactive the program should provide for contractors to receive threat information directly from intelligence sources and in a timely manner. It is suggested that a pilot program be conducted involving contractors, DIS, and intelligence agencies in order to identify threats and assess the possible damage. The results of the pilot program could be used as a base in establishing a viable and realistic threat awareness program.

2. Priority Emphasis on Security of Sensitive Contracts

COMMENT:

Current regulations call for this type of priority emphasis through the assignment of levels of security classification such as Top Secret, Secret, and Confidential in addition to existing caveats such as NATO, COMSEC, CNWDI, and WINTEL which restrict access under specified conditions. However, over the years the practice of "carving out" sensitive programs has been the rule which in most cases relieved DIS of any inspection responsibility. We feel these programs should be classified to the appropriate levels (Top Secret, Secret, and Confidential) depending on the type of contract, i.e. research and development, manufacturing, production, and placed back under the jurisdiction of DISP.

3. Revision of the Industrial Security Manual

COMMENT:

We disagree with this recommendation; however, we do recommend that the ISM be reorganized and restructured to eliminate redundancies multi-references to paragraphs, and unnecessary administrative requirements. This recommended reorganization should be accomplished by Headquarters, DIS, with the assistance of contractor personnel who deal in the day-to-day administration of the DISP. We feel the ISM prescribes the necessary details in order to implement and meet the requirements for the protection of classified information within industry.

4. DIS Inspection of Special Access Programs

a. COMMENT: Concur

b. COMMENT: Concur

c. COMMENT:

We concur with the recommendation to get DIS involved in the security inspection of special access programs and carve-outs. However, criteria and justification for establishing such programs should be rigidly enforced. Those which do qualify as special access programs should then be inspected on a more frequent basis (every four months) by specially trained and briefed DIS inspectors. The inspection criteria should be based on procedures established specifically for special access programs, utilizing the ISM as a guide.

5. Strengthening the Adjudication Process

(Cannot comment without knowing the current adjudication process.)

6. Centralization of the Adjudication Function Within the Department of Defense

(Cannot comment, not knowing the current adjudication process.)

7. Revising the Frequency of Industrial Security Inspections

COMMENT:

We do not concur completely with the elimination of physical inspections of "dormant" and "access only" facilities. We feel these facilities should be visited at least once a year by DIS or have them complete a certification that they do not have physical access to classified material at their location. This could be accomplished on a yearly basis through the mail system. In regard to other cleared facilities, the inspection schedule should be based on the contractor's overall security rating and number of quality security personnel, etc. Most major contractors identified as 1A facilities who have quality programs should only be inspected once a year as long as they conduct the biannual self-inspections.

8. Reporting of All Foreign Travel by Contractor Personnel

COMMENT:

We do not concur with this recommendation on the basis of the administrative burden it would create from the standpoint of cost and time. Also, it would be of questionable intelligence value in that a person making the visit for espionage purposes would deliberately not report it to Security.

9. Creation of Separate Advisor and Inspector Roles of DIS Representatives

COMMENT:

We do not concur with this recommendation in that the inspectors currently fulfill both roles.

10. Establishment of a National Industrial Security Hotline

COMMENT:

We see no need for a "hot line" program in that it serves no useful security purpose. Requirement already exists for employee to report to the security supervisor, FBI, DISCO, DIS offices, on sabotage, subversion, security violation, drugs, alcohol, etc. In addition, such a system would be costly, plus most allegations would be inconclusive and unproductive.

11. Assignment of DIS Personnel to Extremely Complex or Particularly Sensitive Contractor Facilities

COMMENT:

We do not concur with this recommendation. This was tried during Project '60' and failed miserably. We feel it would be a waste of government manpower.

12. Establishment of a Graded Defense Industrial Security Program Inspection Rating System

COMMENT:

We do not concur with this recommendation as written. However, serious consideration should be given by DIS not to list minor administrative infractions corrected during the course of

12. (continued)

the inspection in the "Letter of Requirements" to the Company's Chief Executive Officer. Major problems, of course, should be listed if they indicate a major breakdown of the contractor's program. This should be evaluated on the basis of size of the facility and volume of the classified material.

13. Specialized Training Program for Accrediting Contractor Security Personnel

COMMENT:

This recommendation has merit, especially for the smaller contractors whose security officers have responsibilities other than security.

14. Notification of the DIS of Criminal Investigations Involving Cleared DoD Contractors and Contractor Personnel

COMMENT:

Concur. However, contractors should be notified if it involves one of their employees.

15. Legislative Base for the Defense Industrial Security Program

COMMENT:

We concur in principle; however, the declassification of information involved should depend on the damage to national security.

16. Legislation to Limit Administrative and Judicial Review of DoD Personnel Adjudication to the Adjudicative Procedures Themselves

COMMENT:

We feel this matter should be seriously reviewed.

17. Authority to Suspend and Debar Contractors for Serious Security Infractions

COMMENT:

We feel the current ISM sanctions for unsatisfactory ratings are sufficient.

18. Revised Scope of Personnel Security Investigations

COMMENT:

We concur with this recommendation.

19. Enhancement of Personnel Security Investigative Standards and Reduction of Industrial Clearances

a. COMMENT: We concur.

b. COMMENT: We concur.

c. COMMENT: we concur.

d. COMMENT:

A similar recommendation was made in 1955 and tested. DoD determined the cost and time lost within industry negated the value of the program.

e. COMMENT:

We do not concur with this recommendation on the basis of cost impact to all concerned.

f. COMMENT: We concur with this recommendation.

g. COMMENT:

We do not concur with this recommendation. Would be very costly.

h. COMMENT: We do not concur with this item.

i. COMMENT: We do not concur with this item.

j. COMMENT: We do not concur with this item.

20. Documentation in Standard Practice Procedures Relating to Disciplinary Action for Security Violations

COMMENT:

Hughes Aircraft Company has such a program currently in force.

21. System of Controls Over After-Hours Access and Reproduction Equipment at Cleared Facilities

a. COMMENT:

We do not concur on the basis of cost. Most major contractors have guards on patrol throughout the facility at either two or four-hour intervals.

b. COMMENT:

We do not concur. Would be impractical and costly for large contractors.

22. Access to the Defense Technical Information Center Classified Data

a. No comment.

b. No comment.

23. Proactive Efforts by the DIS to Prevent Unauthorized Disclosures

COMMENT:

Most cleared contractors are in compliance with the requirements of the Industrial Security Manual concerning public releases, etc.

24. Increased Emphasis on Classification Management

a. COMMENT: We concur with this recommendation.

b. COMMENT: We concur with this recommendation.

25. Prevention of "Bootlegging" of Classified Material

COMMENT:

The current procedure within industry of requiring employees to execute DISCO Form 482 (Briefing/Debriefing Statement) covers this recommendation.

SUMMARY OF THE BELL CASE

Our investigation of the Bell case indicated that the incident did not result from a weakness in our security program or classified document accountability system, but from willful security violations by a longtime employee.

Our investigations revealed that William Bell intentionally violated Company and Government security regulations by illegally removing classified documents from company premises. I am sure you will all agree there is no way to prevent such unauthorized removals short of conducting a physical search of each employee as he/she departs company premises.

Our investigation of the incident revealed that the Secret documents charged to Bell were properly accounted for and surrendered by him at the time of his termination.

Concerning Bell's possession of multiple copies of classified documents, this is not an uncommon practice for program managers. Bell, being a program manager, was authorized to request additional copies from Document Control.

Annually, Hughes Aircraft Company conducts a Secret document inventory of all custodians, at which time they are required to justify retention of Secret documents in their possession. In addition, employees are requested to reduce the number of classified documents, and inspections are frequently conducted with the intent of reducing the number of classified documents in the employees' possession.

By Company Bulletin, 29 June 1981, to all Hughes Aircraft Company employees, Dr. Puckett expressed his concern for the Bell incident. He reminded us of the sensitive nature of our work and the absolute necessity of adhering to company security practices.

We believe our security and classified document accountability systems function efficiently and effectively; however, the best system still depends upon the integrity of the individual.

Volume III

STATUS OF THE HUGHES AIRCRAFT COMPANY SECURITY PROGRAM BEFORE AND AFTER WILLIAM H. BELL

In response to the request of the Senate Subcommittee on Investigations concerning the status of the Hughes Aircraft Company Security Program both before and after the William Holden Bell case, the following comments are submitted.

The Hughes Aircraft Company Security Program has always been and continues to be rated as one of the best in the Industry. The details of our program as reported in Volume I, Parts 1. and 2. of our testimony indicate the amount of support and effort given to the implementation of the Defense Industrial Security Program at Hughes Aircraft Company by our top management, security organization, and employees. It is a well-known fact that a successful security program depends on: (1) Reliable and trustworthy employees, (2) An ongoing security education program, and (3) Professional security personnel.

Security is an individual responsibility and contractors must rely on their employees to comply with established security procedures for the protection of classified material.

In an effort to put into perspective the status of the Hughes Aircraft Company Security Program, before and after the Bell case, Attachment I lists in chronological order beginning in 1965 various security education and awareness material which was made available to all employees, including Mr. Bell. The educational material was in the form of articles in our security publication "Security Views," oral briefings by the F.B.I. and other government speakers, at security representatives meetings, noontime movies, new hire indoctrinations, etc. Copies of the articles mentioned above are in Volume I, Part 2 of the testimony.

Also, In July of 1978 our security department reindoctrinated over 30,000 employees at our Greater Los Angeles Area Security Facility. The re-briefing required employees to read and sign a statement indicating their understanding of their individual security responsibilities. Mr. Bell executed this statement on July 29, 1978. It was estimated that in addition to the items listed in Attachment I, Mr. Bell was briefed at least twenty times during his employment by Company and Government security personnel concerning the handling of classified material during the Annual Secret Document Inventory, "696" DoD inspections, and Company self-inspections.

After the Bell case, an in-depth review of the company's security program was conducted. As a result the company strengthened its physical security program by requiring a physical search of all briefcases, packages, and purses carried in and out of company facilities.

Procedures were strengthened and forms revised to control the removal of classified material from company premises.

In 1983, employees were advised through company publications and briefings of the new Industrial Security Manual requirement to report any contact, particularly sustained contact, with a Communist country national, even if purely personal and seemingly casual. In addition, during the F.B.I. briefings and company security representatives meetings, supervision was briefed concerning the "danger signals" which could lead to unauthorized release of classified material.

Attachment I to Volume III,
Chronological Listing of Hughes
Security Education-Awareness-
Training Program

The following are articles, briefings, movies, posters, etc., made available to Hughes Aircraft Company employees from 1965 through 1984. Copies of the Security View Articles are included in Part 2 of Volume I of this testimony.

DATES	SUBJECTS
1965	Inquiries from Soviet Bloc Countries (USAF Security)
1965	Canadians Expose Soviet Spies (AK Bytchkov and C. N. Flouchkin)
1965	"The Spy Next Door" (Movie)
1966	U.S. Airman Held (March Air Force Base), on Charges of Spying for Russia (L.A. Times 31 October 1966)
1966	Industrial Espionage (Brooklyn Federal Court Case)
1966	Navy Serviceman Trapped as Spy (Director of Naval Intelligence)
1967	Industrial Security & Soviet Espionage, Ref: DSA Letter
1967	U.S. Airman Gets Thirty Year Term as Soviet Spy (Photo and Story)
1968	"Air Force Concern" - Telephone Security
1968	Hand-Carrying Classified Information
1968	"Memorandum to Heads of Federal Departments - and Agencies from the President of the United States" on Security & Protection of Classified Information
1969	Handcarrying Classified Material
1970	Protect "NATO" Documents
1970	"New Requirements" for Handcarrying Classified Material
1970	Unauthorized Disclosure of Classified (Industrial Security Letter 27 July 1970)
1971	Foreign Travel, "Defensive Security Briefing"
1971	Use of Self-Service Reproduction Machines
1972	Handcarrying Classified Material
1972	FBI Seizes Russian as Navy Jet Spy (L.A. Times 15 February 1972) Re-print

Hughes Continuing Security Education-
Awareness-Training Program - Continued

DATES	SUBJECTS
1972	Foreign Travel Briefings
1973	Removal of Classified Material to Residence (Strictly Prohibited - Major Violation)
1973	Challenge Visitors - and Red Badges - (Unescorted)
1974	Protection of Classified During Use
1974	Defensive Security Briefings and Foreign Travel
1974	Release of Classified Material to Suppliers/Subcontractors
1975	Classified Document Accountability, "Confidential" included
1975	Shipping and Transmitting Classified Material
1975	Safeguarding Classified During Use
1976	Clearance of Classified and Unclassified Technical Papers
1976	Temporary Loan of Secret Documents
1977	Disciplinary Actions for Security Violations
1977	Classified Intelligence Information
1977	Classified Visits and Handcarrying
1978	*Security Reorientation Program - "Re-Briefing of all employees on their responsibilities"
1978	Transmitting Classified Material
1978	Classified Symposium Attendance
1979	Briefings Required for Handcarrying Classified
1979	Foreign Travel and Defensive Security Briefings
1979	Security Reminders - Drugs, Narcotics, Cameras, etc.
1980	Warning! Intelligence Information - Special Briefings - Counterintelligence Awareness - Defensive Security Briefings

Hughes Continuing Security Education-Awareness-Training Program - Continued

DATES	SUBJECTS
1980	Mailing Classified Material
1980	Signed Receipts for Classified Material
1981	Don't Gamble with Security
1981	COMSEC Requirements
June 1981	Mr. Bell was terminated as an employee of the Hughes Aircraft Company. After his termination the following articles were distributed and briefing given concerning his activities as an employee.
1981-1984	13 articles in the company publications "Security Views"
1981	Special Notices and large poster type enlargement of letters from the Chief Executive Officer Dr. Allen E. Puckett, and 5 Group Vice-Presidents.
1982-1984	FBI Briefings - - Video tape of the Bell case (J. Reid) - Intelligence Threat Briefing for key management personnel (D. Majors) - Foreign Travel - China (Lance Wu) - Counter Intelligence Briefing (D. Majors)
1981-1984	Security Representative Meetings - Emphasis on Espionage - "Espionage" (Film) - Rebriefing Forms - Security Reminders - Distribution of Nation Business acticles on "Soviet Spies"
1984	Special Security Bulletin - Bell case
1984	"KGB" Poster

[illegible]
Zacharski - No Bail

Bell 20 - 271
Zac 9 - 13

Form A. O. 91 (Rev. 12-1-60)

Complaint

United States District Court
FOR THE
CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA
v
WILLIAM HOLDEN BELL,
MARIAN WALTER ZACHARSKI,
aka Marian Wlodzimierz Zacharski

Magistrate's Case No. 81-671M

COMPLAINT for VIOLATION of

U.S.C. Title 18

Section 794(a)(c)

BEFORE JAMES J. PENNE
Name of Magistrate

Los Angeles, California
Address of Magistrate

The undersigned complainant being duly sworn states that:

That beginning or before February 1978 and continuing to on or about June 28, 1981, in Los Angeles County within the CENTRAL District of CALIFORNIA,

(1) WILLIAM HOLDEN BELL and MARIAN WALTER ZACHARSKI aka Marian Wlodzimierz Zacharski

XXX and others unknown did unlawfully, knowingly and wilfully conspire and agree to communicate, deliver and transmit to a foreign government, to wit, Polish People's Republic, and representatives, officers, and agents thereof, information relating to the national defense of the United States with intent and reason to believe that the said information would be used to the advantage of said foreign nation, to wit, Polish People's Republic.

The objects of said conspiracy were to be accomplished as follows:

Defendant WILLIAM HOLDEN BELL would procure classified, secret information relating to the national defense of the United States and deliver said information to agents of Polish People's Republic. In return for this information defendant MARIAN W. ZACHARSKI would make regular payments of cash and/or gold coins to defendant WILLIAM HOLDEN BELL.

To effect the objects of said conspiracy, the above named defendants committed various overt acts within the Central District of California including but not limited to the following:

1. In April 1981, defendant WILLIAM HOLDEN BELL travelled to Switzerland from Los Angeles, CA.
2. In May 1981, defendant WILLIAM HOLDEN BELL met with defendant MARIAN W. ZACHARSKI in Los Angeles, CA.
3. On June 28, 1981, defendant WILLIAM HOLDEN BELL met with defendant MARIAN W. ZACHARSKI in Los Angeles, CA.

(SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED AS PART OF THIS COMPLAINT)

Signature of Complainant.
GEORGE S. BACON
Special Agent, FBI
Official Title.

Sworn to before me, and subscribed in my presence, June 29, 1981.

United States Magistrate.

RSB:gd:gad REC:$ No Bail (Zacharski)
$100,000 CS/AB w/10%
dep. (Bell)

(1) Insert name of accused
(2) Insert statement of the essential facts constituting the offense charged

AFFIDAVIT

I, GEORGE S. BACON, being duly sworn, hereby depose and say:

1. I am a Special Agent for the Federal Bureau of Investigation currently assigned to an Espionage Squad of the Los Angeles Division. I have been a Special Agent since 1963 and have been assigned to the investigation of espionage matters since 1965.

2. This affidavit is made in support of a complaint against WILLIAM HOLDEN BELL and MARIAN W. ZACHARSKI for a violation of Title 18, United States Code, Section 794(a)(c), to wit: Conspiracy to gather and/or deliver defense information to aid a foreign government.

3. In early 1979, I received information that classified documents in the custody of the Hughes Aircraft Company (HAC), El Segundo, California, had been transmitted to agents of a foreign government, to wit: Polish People's Republic. Subsequent investigation determine that WILLIAM HOLDEN BELL, an employee of HAC, should be considered a suspect in the transmission of these documents to agents of the Polish government.

4. On June 23, 1981, WILLIAM HOLDEN BELL was interviewed and provided a signed statement admitting complicity in the theft of classified documents from HAC and the delivery of these documents to MARIAN ZACHARSKI, an official of the Polish American Machinery Company, and other agents of the Polish government. He said he is currently employed as a Project Manager at HAC, Radar Systems Group, Building R1, El Segundo, California, and holds a "Secret" clearance. He said beginning in late 1977 or early 1978, he met MARIAN W. ZACHARSKI who was residing in the same apartment complex where he (BELL) resided. He said he and ZACHARSKI developed a friendship.

He said that at that time he was having some financial difficulties and ZACHARSKI told him he might be able to assist him in getting out of those difficulties. ZACHARSKI told him he would like to obtain various documents which were in the possession of HAC and he would be willing to pay for anything which proved of value. BELL told me he only obtained unclassified material in the beginning but realized when he took a payment from ZACHARSKI he would be in a compromising situation and would be required to obtain other documents of higher classifications. BELL said the first payment which he received from ZACHARSKI in late 1978 or early 1979, was $5,000 and several weeks later he received a second payment of approximately $7,000. BELL said these two payments of $5,000 and $7,000 were made to him in the condominium complex area. BELL said he continued to supply ZACHARSKI with classified information and at one point ZACHARSKI gave him a special motion picture camera, capable of taking single frame exposures, a tripod, and "special" film. BELL has provided these items to the FBI. BELL said this camera, tripod, and film were given to him by ZACHARSKI within the condominium complex. BELL said that on or about September 1979, ZACHARSKI instructed him it would be necessary for BELL to start making periodic trips to Europe in order to deliver the film to agents of the Polish government, overseas. BELL said this ended all document exchange between he and ZACHARSKI. BELL said that on or about November 1979, he took his first trip to Austria, where he met with agents of the Polish government (hereinafter "Polish agents"). BELL said that ZACHARSKI had instructed him to go to Austria and how he would be contacted while in Austria. BELL said ZACHARSKI told him he would be met by someone who would ask him, "Aren't you a friend of Marian?" On June 27, 1981, Special Agent James R. Pace, who is a Special Agent of the FBI, assigned to the Espionage Squad, and who interviewed WILLIAM HOLDEN BELL on June 23, 24, 25, 26, and 27, 1981, told me that shortly before BELL's trip to Austria, ZACHARSKI requested that BELL give him (ZACHARSKI) a photograph of BELL. BELL did so. BELL said he was met by three people who used the above expression and he delivered to them the film of the documents he had photographed and taken on the trip. BELL said that at that first meeting he delivered a total of four rolls of film to the Polish agents. BELL said that it was at this first meeting with these Polish agents that the manner and type of payment he would receive was discussed. He said he and the Polish agents agreed that he would be paid $3,000 a month in U. S. currency plus a lump sum payment of $60,000 a year, with the form of the lump sum payment undecided. BELL said they agreed he would also receive approximately $3,000 to $5,000 for any expenses he incurred during his trips to meet with the Polish agents. BELL said the meeting ended when he was instructed by the Polish agents to return to Europe in May 1980, and was given a general description of HAC information he was to bring with him to the next meeting.

5. BELL said that in May 1980, as instructed, he traveled to Austria, and met two of the agents he had met with in November 1979, and delivered to them film which contained portions of the HAC document classified "Secret." In a subsequent interview on June 26, 1981, I showed BELL an HAC document entitled "Low Probability of Intercept Radar Phase I, Final Report," which is classified "Secret." BELL identified the five pages of that document, all classified "Secret," which he photographed and gave to

the Polish agents

6. BELL said that during this second trip he was told by the Polish agents that he would be paid the $60,000 a year lump sum payment in the form of gold coins. On June 27, 1981, Special Agent Eugene B. McCarthy, who is a Special Agent of the FBI, assigned to the Espionage Squad, and who interviewed WILLIAM HOLDEN BELL on June 24, 25, 26, and 27, 1981, told me that BELL had told him that he had been instructed by the Polish agents overseas that he was to discontinue receiving payment in all forms from MARIAN ZACHARSKI. In the early summer of 1980, BELL was told by ZACHARSKI that he, ZACHARSKI, would continue to make monthly payments to BELL. Since that conversation with ZACHARSKI, BELL said he has received monthly payments from ZACHARSKI of approximately $3,000 per month in U. S. currency through May 1981. In addition to monthly payments of currency, BELL said he also received, on an irregular basis, payments from ZACHARSKI in gold coins. BELL said ZACHARSKI always made the payments to him within the condominium complex.

7. BELL said he went to Austria, in October 1980, as he was instructed at the meeting in May 1980. He said he met with one of the Polish agents that he had met with before. He delivered film to him and received approximately $7,000 in U. S. $100 bills. BELL said he had photographed two HAC documents, each classified "Secret." On June 26, 1981, I displayed to BELL two HAC documents classified "Secret," one entitled "Covert All Weather Gun System (CAWGS), Technology Demonstration Program, Volume II - Technical Proposal" and the second entitled "Covert All Weather Gun System (CAWGS), Volume II - Technical Proposal," which BELL identified as documents he photographed in their entirety and delivered to the

Polish agent at this meeting. BELL said that he and the Polish agent also discussed when the next meeting would take place, how they would meet and what documents the Polish agent was interested in. BELL said the next meeting was scheduled for April 1981 in Switzerland.

8. BELL told me that in April 1981, he went to Switzerland as instructed, and again met with the Polish agent. He said he gave this agent some film of a HAC document classified "Secret" and received approximately $5,500 from the man. On June 26, 1981, I exhibited a HAC document classified "Secret" to BELL. This document is entitled "Dual Purpose Weapon System (DPWS), Study Effort." BELL told me that he photographed this document in its entirety and delivered it to the Polish agent in Switzerland.

9. On June 27, 1981, I interviewed James K. Easton who told me he is the Assistant Division Manager of the Advanced Programs Division of the Radar Systems Group, HAC, El Segundo, California. He said that he is WILLIAM HOLDEN BELL's immediate supervisor and that BELL holds a security clearance for information classified "Secret." I showed him the four HAC documents classified "Secret" which are described above. He told me that each document was properly classified and remains classified. He told me the information contained in these documents relates to the national defense of the United States. He also told me that the unauthorized disclosure of the information contained in these documents to agents of a foreign nation could have serious consequences to the national security and would be of advantage to a foreign nation.

10. On June 28, 1981, I was told by Special Agent James B. Reid the following transpired on June 28, 1981:

a. At approximately 8:30 A. M., BELL had been wired by a Special Agent with a Nagra SNST voice recording system.

b. At approximately 9:00 A. M., ZACHARSKI was seen entering his apartment.

c. At approximately 9:30 A. M., ZACHARSKI knocked on BELL's apartment door and the two of them exited to talk.

11. On June 29, 1981, at approximately 10:30 A. M., I listened to a tape recording of the conversation that transpired between BELL and ZACHARSKI. This conversation occurred at approximately 9:30 A. M. on June 28, 1981. I immediately recognized BELL's voice on the tape and at one point in the tape, BELL referred to ZACHARSKI by his first name: MARIAN. In the conversation I heard the following:

a. BELL asked ZACHARSKI if it was safe "to talk here" and ZACHARSKI said it was.

b. BELL told ZACHARSKI that he (BELL) is working on a new program and gathering several secret documents together to be filmed.

c. BELL told ZACHARSKI that he did not want to be paid in gold on the next trip and ZACHARSKI said "no problem."

d. BELL asked ZACHARSKI if he (BELL) had already provided secret documents on a particular project and ZACHARSKI said "partially."

/

/

/

/

/

e. ZACHARSKI asked BELL if he had enough film, to which BELL replied that he did.

GEORGE S. BACON
Special Agent
FBI

SUBSCRIBED AND SWORN to before me
this _____ day of June, 1981.

UNITED STATES MAGISTRATE

RESPONSES TO QUESTIONS SUBMITTED BY THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS ON FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

8 May 1985

RICHARD M. WELBY
HUGHES AIRCRAFT COMPANY

1. Q. Both William Bell and Ruby Schuler had secret clearances based only on a National Agency Check. Bell claimed his secret clearance hadn't been updated in 28 years?

True. Mr. Bell's clearance hadn't been updated in twenty-eight years in that there is no current DoD requirement for updates of Secret clearances.

Should the present investigative scope of secret clearance be expanded?

Yes

How?

Require a personal security interview similar to the one conducted for Top Secret clearances.

2. Q. Do you feel that present government policy should be changed to permit the granting or continued holding of a security clearance be a condition of employment?

Yes

3. Q. Do you feel that contractor security personnel should have access to the privacy portions of clearance applications?

Yes

4. Q. Should DOD required security controls be enhanced during non-working hours at cleared Defense contractors authorized to store classified material on the premises?

Current ISM requirements provide more than enough after-hour security controls. (At large contractor facilities, twenty-four hour perimeter controls and bi-hourly guard patrols are maintained.)

5. Q. In each of the three cases which you are familiar with, the William Holden Bell case at Hughes, the Harper-Schuler case at SCT, and the Christopher Boyce case at TRW, extensive classified information was lost. Yet in none of them were the contractors themselves held accountable in any way for the breaches in security. No fines were levied, no disciplinary action was taken, no contracts were lost. Critics of the current system say that is wrong, that contractors should be held accountable for security failures. If the contractors were held accountable to some extent for the conduct of their employees, might that not result in increased security in the defense industries?

No, we feel the current sanctions placed on contractors for deficiencies found by DIS during "696" security inspections are sufficient in that contractors are obligated to correct the cited major deficiencies within thirty days or become ineligible to receive classified contracts.

6. Q. In your opinion, what is the biggest problem with our current personnel security program?

Strengthening the contractor requirement for granting Confidential clearances.

7. Q. Do security protection standards for the handling of classified material vary between government and industry? If so, does this pose a problem to industry?

Yes, contractors are required to maintain a system for a continuous chain (individual to individual) of receipts for all Top Secret and Secret documents. The Department of Defense also requires a continuous chain of receipts (individual to individual) for Top Secret documents but only requires receipts for Secret documents which are transmitted out of the DoD activity to other government activities and contractors (DoD Directive 5220.1R, Paragraph 8-202).

8. Q. Should DIS establish a nationwide security hotline for receipt of anonymous information (6(b)(1) of the Industrial Security Manual) impacting on the Defense Industrial Security Program?

No. In our opinion the establishment of a nationwide security "hotline" would be costly and serve no useful security purpose.

9. Q. Should the inspection rating system be changed from satisfactory/unsatisfactory to a graded system such as outstanding, superior, satisfactory, marginal, and unsatisfactory?

No. We feel the current system of rating is satisfactory.

10. Q. In many "carve out" contracts an award provision for security is utilized. What are your feelings about such a proposal for Secret and particularly sensitive DoD contracts?

I feel this issue has considerable merit and should be reviewed further.

11. Q. Mr. Welby, if it is true that William H. Bell was deficient in both his awareness of the hostile intelligence threat and his grasp of security requirements while employed at Hughes Aircraft, what measures has Hughes taken to improve its security education awareness program for other cleared employees?

If Mr. Bell was deficient in his awareness of the hostile intelligence threat and his grasp of security requirements at Hughes, it was through his own doing. Mr. Bell, like all cleared Hughes employees, received indoctrinations, briefings, and written educational material on hostile intelligence threats, espionage, foreign travel requirements and restrictions concerning unauthorized reproduction, handcarrying, and taking classified material home.

From 1965 to 1981 Hughes employees, including Mr. Bell, were provided with educational information concerning espionage and the hostile intelligence threat (22 times), foreign travel (13 times), reproduction restrictions (10 times), handcarry procedures (24 times) and the prohibition of taking classified material home (7 times). This was in addition to personal contacts by company and government security personnel during inspections, document inventories, and handcarry briefings, etc.

11. (continued)

The company has an ongoing security education and awareness program which highlights the hostile intelligence threat (See Attachment VI, Volume 1, Part 2, entitled "Security Education at Hughes" of my testimony.)

12. Q. Should fulltime DIS representatives be assigned to contractor facilities, as recommended by the DoD Harper Report?

No. It is my understanding that this concept was tried during the sixties ("Project 60") when the Defense Contract Management Regions were being formed. Result of that attempt proved to be costly, counterproductive and as a result was discontinued.

13. Q. Do you have any recommendations for legislative action which would enhance personnel security?

Yes. Permit contractor security personnel to have access to the privacy portions of the clearance application and strengthen the contractor requirement for granting Confidential clearances.

14. Q. Would you furnish a copy of the number of 6(b)(1) violations reported by your company for the last five (5) years?

Our records reflect that 215 6(b)(1) reports were submitted to the government by Hughes Aircraft Company's cleared facilities from 1982 through April 30, 1985.

Senator NUNN. Before we close, I would like to note that there was an article in USA Today that states, "Senators Say Security System is Lax." Nothing wrong with the headline. The picture is not too good, but none of mine are. The article said in the first paragraph, "The Government hands out too many security clearances—especially to immigrants from communist countries—two Senators said today." Those are not quotes, but many people, when reading, don't understand that we didn't say that. That is what somebody sitting here surmised.

It goes on to identify Senator Gore and myself. The rest of the article is fine. The part that I really want to direct a couple comments to is within the dashes, "especially to immigrants from communist countries." Neither Senator Gore nor I said that. We did go into the number of clearances we have in that area. The reason we went into the number is obvious because of the lack of access that the agencies have to do background checks abroad.

We have gone into considerable detail about the difficulty of background checks in this country. Background checks are extremely difficult in any foreign country and certainly those in closed societies, not just communist societies, but any closed society are more compounded and difficult. But I wanted to clarify this because this issue has to do with the ability of the Government to conduct personnel security investigations into the backgrounds of immigrant aliens and recently naturalized citizens who apply for clearances.

Our principal concern is that our Government is unable to verify many of the assertions immigrant aliens make about their past in the personnel security questionnaires. This is particularly true in closed-society countries. We have had the case of Veliotis that we have gone into. Of course, Greece is not a closed society. Greece is part of our NATO Alliance. We saw the great difficulty there in that case I want to emphasize the problem is not with immigrant aliens coming into this country. It is not because we don't welcome them when they come in under legal procedures. The problem is the Government's apparent difficulty in conducting effective personnel security background investigations.

We did go over the numbers. That was not done critically. It was done to emphasize the extreme difficulty these agencies have because while we are critical of the agencies, when we think criticism is due, we also think it is important for the public and for the other parts of Government and for the Congress to understand the extreme difficulty the Defense Investigative Service has, the FBI has, the Office of Personnel Management has, the CIA occasionally has, when they get involved. This is an enormously difficult problem in a free society, and we do not in any way advocate giving up that cherished freedom to deal with the problem. We would rather have security breaches than lose those freedoms, although what we try to do is draw a balance to determine whether we can improve our security without in any way jeopardizing our freedoms in this country. We certainly would not jeopardize one of the most prized freedoms that we have, that is the freedom of people to come into this country and become citizens under the legal process.

And, I might add, some of our most valuable citizens historically have come via immigration. Certainly some of our most valuable, loyal, dedicated, and talented Americans have come here from behind the Iron Curtain and from, indeed, other closed societies. We value them coming into this country. We value their citizenship. We are indebted to them for the role they have played in developing this country and many of them play a very key role in national security.

That doesn't obviate the problem, but it does mean when you see an article like this that takes the whole thing out of total context and highlights something that was not said by either Senator Gore or myself, I think I have to call attention to it.

USA Today probably doesn't have anybody here today, and certainly they do a good job on most things. I just wanted to point that out. I think it is enormously important these hearings not be misinterpreted on that point.

Senator GORE. Would the Senator yield on that point? I would just associate myself with your remarks and add I certainly wish an immigrant from the Soviet Union loyal to his new country of the United States was hired instead of the Californian, Chris Boyce, in that sensitive position. I think the number of immigrants from behind the Iron Curtain were used among several statistics to illustrate the scope of the problem and not to single out immigrants.

Everyone is aware of the Soviet espionage effort and some of the techniques used, and it's obvious this serves as no illustration of why we have to make greater efforts. There are many other illustrations as the Boyce case and others illustrate.

I would just associate myself with your remarks.

Senator NUNN. I would ask staff to get a copy of my remarks—yours and mine—and give it to the USA Today people. It is a fine newspaper. We do have to point out sometimes the erroneous for self-protection, and also to protect the purpose and scope of this hearing which I think has been very helpful.

Senator GORE. You are not going to complain about the picture, are you?

Senator NUNN. I can't complain about that. Unfortunately, it looks like me. That's the problem. The hearing record will remain open for 10 days for exhibits and other answers. General Pauly, you indicated you have others for the record. We will keep the hearing record open for that period of time. If that presses you, let us know and we will be flexible on that.

We will announce another date for General Stilwell and his associates to appear. Thank you all for being here. The hearing will be in recess.

[Whereupon, at 1:25 p.m., the subcommittee recessed to reconvene at the call of the Chair.]

FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

THURSDAY, APRIL 25, 1985

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The subcommittee met at 10:09 a.m., in room SD-342, Dirksen Senate Office Building, under authority of Senate Resolution 85, section 13, dated Feb. 28, 1985, Hon. William V. Roth, Jr., chairman of the subcommittee, presiding.

Members of the subcommittee present: Senator William V. Roth, Jr., Republican, Delaware; Senator Sam Nunn, Democrat, Georgia; and Senator John Glenn, Democrat, Ohio.

Members of the professional staff present: Daniel F. Rinzel, chief counsel; Eleanore J. Hill, chief counsel to the minority; Katherine C. Bidden, chief clerk; John F. Sopko, assistant counsel to the minority; David Glendinning, staff counsel; Leonard A. Willis, Glenn W. Fry, and Fred Asselin, investigators for the minority; Sarah Presgrave, executive assistant to the chief counsel; and Kathleen A. Dias, executive secretary to the chief counsel to the minority.

[Senators present at the convening of the hearing: Senators Roth and Nunn.]

Chairman ROTH. Today the permanent subcommittee will conclude its hearings on the Government personnel security system. We are very pleased to have today as our sole witness Gen. Richard Stilwell, Deputy Under Secretary of Defense for Policy, responsible for implementation of policy and procedures for the Defense Personnel Security Program.

General Stilwell, as you may know, we have a rule of this subcommittee that everyone has to be sworn who testifies. So we would appreciate it if you and your colleagues, if they are going to testify, stand and raise your right hand.

Do you swear the testimony you are about to give will be the truth, the whole truth and nothing but the truth, so help you God?

General STILWELL. I do.

Mr. SNIDER. I do.

Mr. FEDOR. I do.

Chairman ROTH. Thank you. Please be seated. Senator Nunn.

Senator NUNN. Mr. Chairman, I will have something to say at the close, but let me say at the outset that I look forward to exploring with our witnesses this morning some of the things we learned in the last 4 or 5 days. I want to thank General Stilwell, Britt

Snider, and Bill Fedor for being patient with us. We did not get to them last week when we were wrapping up, and they had been here all morning. We thank you very much for allowing us to have this hearing this morning. We are all in a better position to analyze the issues today than we would have been at the very end of that hearing late in the day. It did require a great deal of cooperation from the witnesses, and we appreciate it very much, indeed. I look forward to hearing the testimony.

Chairman ROTH. General Stilwell, will you please proceed?

TESTIMONY OF GEN. RICHARD G. STILWELL, USA (RETIRED), DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY, ACCOMPANIED BY L. BRITT SNIDER, DIRECTOR, COUNTERINTELLIGENCE AND SECURITY POLICY, DEPARTMENT OF DEFENSE; WILLIAM R. FEDOR, DEPUTY DIRECTOR, COUNTERINTELLIGENCE AND INVESTIGATIVE PROGRAMS; AND KATHLEEN A BUCK, ASSISTANT GENERAL COUNSEL, DEPARTMENT OF DEFENSE

General STILWELL. Thank you, Mr. Chairman. May I extend, with your permission, the list of backup witnesses to include a very splendid lady and very competent Government official, the assistant defense counsel, general counsel, Ms. Kathleen Buck who is in the back of the room.

Senator NUNN. I would like to ask her to come up and join you at the table. I do not know if we are going to ask her questions. She has already helped us great deal and submitted testimony as part of the record. So we would welcome you being here.

Chairman ROTH. Do you swear the testimony you are about to give will be the truth, the whole truth and nothing by the truth, so help you God?

Ms. BUCK. Yes, sir; I do.

Chairman ROTH. Thank you, and we are delighted to have you.

General STILWELL. Mr. Chairman, my prepared statement is submitted for the record.

Chairman ROTH. Thank you. It will be included in its entirety.

General STILWELL. It would be ill use of your time and Senator Nunn's to even summarize it, but I ask your indulgence for a few opening remarks.

First, let me compliment your subcommittee and your staff which has made such exhaustive preparations for the initiative in holding hearings on this key aspect of national security. The documentation assembled, the prepared statements, the transcripts and the answers submitted for the record will combine into a uniquely valuable document for all who have responsibilities for or interest in personnel security.

For the past 4 years, my staff responsibility for DOD security policy and supervision of the Defense Investigative Service has been part of my diversified portfolio, and I have slept less comfortably as a result, aware that personnel security is the most tenuous link in the complex activities designed to protect the national security.

I assess that I have discharged that responsibility with only indifferent success. From this experience, I have distilled a few conclusions.

First, the overall security objective is the protection of classified information. Thus, the first step in a coherent cost-effective system to accomplish that is to assure that we classify only what needs to be classified because the totality of classified information scopes the problem.

We have an estimate that last year the Department of Defense created 16 million new items of secret correspondence. The classification rules are sound, but in the application, must err on the side of caution. My favorite quote from Clausewitz is, "In strategy, everything is simple but not on that account easy."

[At this point in the hearing, Senator Glenn entered the hearing room.]

General STILWELL. What I believe he meant was that the formulation of strategy or policy is about 2 percent of the total challenge, the tough part being the implementation.

Second, a request for security clearance should be linked to a need for access. It's our visceral view that there is a great disparity between the number being cleared and the number being accessed. The Harper Committee estimated, and I underscore "estimated," that about one-third of the contractor employees cleared for top secret never saw a top-secret document. But the point is that we have no accurate statistics to confirm the gap between cleared personnel and those having access.

My successors must work to get these statistics. A related point, Mr. Chairman, is that clearance at secret or higher level does not, per se, authorize access to all information at that classification level, but only the segment that he or she needs to know for the performance of duty. The larger the cleared pool, the more likely violation of the need-to-know principle.

Third, initial investigation of an individual's trustworthiness is important because it is currently the only basis for prediction of future behavior. However, it is no assurance that he or she will thereafter handle stresses, strains or temptations.

Personnel security is a function of command and management and individuals must be subjected to continued monitoring, and periodic evaluation by their superiors.

To my knowledge, we do this in a structured and disciplined way only under the Defense Personnel Reliability Program with respect to personnel in nuclear weapons units. I can further elaborate on this point, if you desire.

Based on these comments, I see the principal challenges both within DOD itself and the defense industrial complex to be first a tighter process for validating requests for security clearance to the end of a substantial reduction in new requests and the continuation in effect of those already issued. This is the precondition to expansion of secret investigation procedures which we all recognize to be adequate.

Unless and until this is accomplished, we cannot in good conscience go to the Secretary of Defense with a request for greatly expanded investigative resources and assure the Secretary that provision of such resources would be a wise, efficient diversion in an already constrained budget.

Second, reduction in numbers would permit a greater focus of available resources on reinvestigation of those individuals with continuing access and, therefore, the more vulnerable. Such reinvestigations should be prioritized in accordance with the sensitivity of the information to which accessed.

Third, and this, in my view, is a particular moment, we need to assiduously pursue research into the personnel security field, much along the lines annunciated by Dr. Flyer in his very excellent statement, with the objective of gaining better tools for predetermining motivation and analysis of behavior displayed by individuals who have or being considered for clearance and access.

And, finally, sir, we must stress, restress and stress again the continuing assessment of human reliability as an inherent function of command and management, with security inspections focusing more on the individual and security awareness and job satisfaction than unlocked safes and windows.

This concludes my opening comments. I am ready for your questions.

Chairman ROTH. Thank you, General Stilwell. I am going to call first upon Senator Nunn for any questions he may have.

Senator NUNN. Thank you very much, Mr. Chairman. First, let me say to General Stilwell, that he has been an outstanding military leader and public servant for a long, long time, not just in his most recent job. I first met him when he was in Korea and have stayed in close touch with him since then. He was of tremendous benefit to me when I made a study of some proposal being made about Korea, troop commitments, so forth. He has always been cooperative. We haven't always agreed on every detail, but I found him to be a man of great integrity and I greatly value what he has done for the U.S. Army, for the Department of Defense and for the national security of our country. He is recently retired, but I hope we will continue to be beneficiaries of his expertise, wisdom, and good, sound advice.

General, I appreciate your summary today. Your statement is all worthy of very careful attention, which I have already given it. We have, I think, a major challenge. Although I knew the problem was large before we started these hearings, the scope of the problem and the order of priorities, which you have just laid out, I think, is now much clearer. I think your priorities, which as you said, we need to come to grips with, are certainly in line with my thinking. I hope we can devise a set of recommendations based on these hearings. Senator Roth and myself and others, Senator Glenn and Senator Gore and others who participated—Senator Rudman—that will be the initial sounding board for perhaps some reaction from the executive branch I hope between these hearings and the legislative recommendations and the executive branch we will be able to come up with some things that will really do some good in improving this overall area.

I have a few questions, and then I will yield to Senator Roth for whatever questions he has. If you had to outline the problems, the major problems in personnel security now in capsule form, say the top three problems, what would they be?

General STILWELL. Well, I would repeat, Mr. Senator, the core of the problem is the overall scope of national security relevant classified information that we are designed and directed and dedicated to protect. These are not independent of one another, but we must continue to take action to get better control over the classification management of the process and the amount of material being circulated that is classified that may not need to be classified because to the extent that you are clearing people to handle material that doesn't need to be classified in the first place, you are diverting resources.

I realize it is easy to say that, but throughout the departments, or course, you have an expanding, continually expanding requirement of requests for clearance.

The collateral aspect of that, however, is that, and almost the equivalent problem is a better assurance that we are only clearing people who need to be accessed to the information, and there is where I believe we can make substantial progress. It won't be easy.

Senator NUNN. No. 2 is easier than No. 1, would you say, to deal with?

General STILWELL. Yes.

Senator NUNN. Although both are tough.

General STILWELL. Both are very, very difficult.

Senator NUNN. But the first one being a subjective judgment by thousands and thousands of people.

General STILWELL. Exactly.

Senator NUNN. I don't see how you legislate the first one. There may be an answer. By legislate, I mean even legislation or regulation by the executive branch.

General STILWELL. It is difficult to legislate both, sir, but you are quite right, sir; quite right. The second one, in turn, will be difficult and requires a very disciplined reaction because as I think prior testimony may have indicated, there are procedures which really kind of encourage contractors to have a large pool of cleared people.

Senator NUNN. On that first point, and I will come back, I was at a briefing not long ago and each one of the charts had the classification up there. There was one chart—this is obviously military organizations—it had up there these words: "We must not fail." And it was classified as secret. Of course, we asked the question why. Nobody could give an answer, but the answer is, when you are classifying a whole lot of things, you tend to classify everything. Where do you draw the line?

Senator GLENN. We want to keep them guessing. We don't want them to know we don't want to fail. [Laughter.]

Senator NUNN. Those two points that you make, is there anything that you know of that can be done in terms of any provisions to law that need changing to address either one of these two points that you know of?

General STILWELL. No, sir; as we said at the outset the definition of the various categories of security are reasonably clear. I don't know if manipulating those words is going to help. It is in the interpretation you have the problem. So it simply requires education, discipline, perhaps occasionally a department head can demand a percentile reduction or something like that. Continuing effort to review documents that are extant to remove the classification from them, if they no longer meet the criteria, but I don't see how we can legislate anything with respect to the business of no request for clearance unless access is required on a continuing basis by the time the clearance is established.

There is one area that we have considered some aspects of. We can do more, in my view, to find a methodology that would facilitate a one-time upgrade of a security level for an individual who needs one-time access to a document at a higher level.

Senator NUNN. Rather than going through the whole procedure?

General STILWELL. Yes, sir. There is some money, in my view, to be made in relooking at that whole area as to how we can do that.

Senator NUNN. A while ago you were talking about the number of people who had access, but never were exposed to classified information. Would there be a way to give discretion to a group of supervisors or project managers, or at some appropriate level, that might vary from program to program, so that if a person needed access for just one document, that that would be done on an ad hoc, delegated basis requiring a signature or statement that this is being done because of certain circumstances. You could let him sign a statement saying this is the only document that we will have access to. Is that what you have in mind rather than going through the whole process to upgrade to top secret?

General STILWELL. Yes, sir; I think I would continue to centralize that at the regional offices of the Defense Investigative Service, but it would have to be the same man, company X—let's say Lockheed in the Sunnyvale area—clearance in the San Francisco office; they have one case they need access for a particular piece of technical data, whatever. He has it for a prescribed period of time and for that only.

Senator NUNN. I think you would have to have an expedited process that did not take any time. Otherwise there would be an incentive to keep going the way they are now and get everybody possible cleared.

General STILWELL. There wouldn't be any clearance. There wouldn't be any additional clearance. You would just access them.

Senator NUNN. I think whoever approved it at whatever level, it would have to be done in an expeditious fashion.

General STILWELL. Yes, sir.

Senator NUNN. You can really channel it through and do it quickly. How about a need for revising Executive orders? Do we need to have a whole revision of Executive orders? It has been a long time since those have been revised. I know they have been updated somewhat. Is there a need for a comprehensive review of that?

[At this point in the hearing, Chairman Roth withdrew.]

General STILWELL. As I believe the subcommittee is aware, sir, there is a department initiative in progress as part of the President's National Security Directive 84 to develop a new Executive order confined to security only in contradiction to the one Executive Order 10450 which deals tangentially with security as well as suitability. The new order would establish, according to the guidelines for most of the departments and agencies affected, a uniform standard across the executive branch for civilians, for military, and for contractors.

We think that that is a very important requirement to be met.

Senator Nunn. So you would have uniformity?

General Stilwell. Yes, sir.

Senator Nunn. We understand and heard in previous testimony that the Presidentially directed interagency effort was to have reviewed and did some reviewing of Federal personnel policies and issued a set of options to NSC. We heard that it has been about a year since that happened and nothing else has happened. It looks like that effort is bogged down. Do you want to comment on that as to whether it is bogged down and, if so, why?

General Stilwell. Sir, since the recommendations put forward a good many months ago with unanimity on the part of my interagency group which helped Ms. Lawton prepare them, you have to say it is temporarily in a hold basket, for reasons——

Senator Nunn [interposing]. Is that a synonym for "bogged down"? Now that you are retired.

General Stilwell. Yes, sir; I would say the dictionary would consider that as a substitute, with comparable meaning. I suppose it's a question of priorities. I was presumptuous enough some months ago to write a little note saying we ought to get on with this. I do not believe, but I am not totally informed, that there is a substantive problem. We will continue to do what we can within our limits to move that forward because there were some very straightforward recommendations which, if approved, would permit that interagency group to move out smartly with a new Executive order dealing with personnel security only which would establish common standards across the executive branch which would also establish more uniform adjudication standards throughout. That's all.

Senator Nunn. Who does the Department of Defense look to for guidance in the personnel security area, other than the President of the United States himself? Is there any other agency or group of people that hands down policy guides to the Department of Defense, or is this a responsibility of the Department of Defense itself, subject to the President?

General Stilwell. In the area of sensitive compartmented information, we look to the Director of the Central Intelligence for guidance because under both the National Security Act and the current Executive Order 12333, he is charged with the development of common standards for the protection of sensitive compartmented information; primarily that is a question of consensus. So we march to that drummer, Mr. Chairman.

Other than that, there is no national office that provides across-the-board guidance for the remaining categories of security. The Secretary depends on his general authority rooted in the National Security Act for that.

Senator Nunn. Do you see a need for some type of arrangement that would have something comparable to information security oversight in the personnel area? Is there a need for a Federal personnel security program that would be under the direction of one overall centralized source?

General STILWELL. I would see something comparable to the ISOO as the concomitant of an Executive order which would deal with those items which we just mentioned that are under consideration in NSDD-84. So that if you have a common standard across, then I would see some office like the ISOO, although unlike the ISOO, I would think that would be under the aegis of the National Security Council itself.

[At this point in the hearing, Chairman Roth reentered the hearing room.]

Senator NUNN. Do any of the other witnesses want to comment on that at this juncture?

Ms. BUCK. I would have one comment, Senator, and that is I think on the legal side that we have been able to work with the General Counsel of the Office of Personnel Management and the Department of Justice, specifically to look to the Department of Justice to more or less coordinate legal actions in the entire executive branch on security clearance matters.

Senator NUNN. You say that is not being done now?

Ms. BUCK. We are doing that on the legal side; yes.

Mr. FEDOR. I would add, Senator Nunn, that part of the charter of the NSDD-84 study group is not only the need for personnel security policies and procedures, but the question of national authority and that would certainly be one of the subjects discussed when the group reconvenes as to where that national authority should lie.

I would agree with General Stilwell the appropriate place would come under the National Security Council.

Senator NUNN. Where would the Office of Personnel Management fit into this scheme?

General STILWELL. The Office of Personnel Management, of course, has its very, very important function derivative from the Civil Service Commission in the whole field of standards for and preconditions for Federal employment.

[At this point in the hearing, Chairman Roth withdrew from the hearing room.]

General STILWELL. I am not the expert on this, but it seems to me they are very clear, but the Executive order we have in mind would make a clear distinction between that portion of the Executive order which applies to the OPM with respect to employment, suitability for employment and the security standards.

Senator NUNN. One other question and then I will yield to Senator Glenn. I will come back after Senator Glenn has asked his questions, and ask a few more.

We had testimony by Donald Devine that the National Security Council, through the SIG(I) process, has already ruled by implication, by silence I suppose, on the recommendations made by the NSDD. Would you agree with that interpretation? He didn't say all of them, but he said there were those that—the areas that related to his jurisdiction he felt by silence that the NSC had, in effect, acquiesced and approved those recommendations that were set forth, as I understand it, in policy terms, option terms.

General STILWELL. To give you the full process, the policy options and the preferred options were developed first by an element of the Interagency Group Countermeasures which I chair. The recommendations there were approved by my group for transmittal to the Senior Interagency Group for Intelligence, which Mr. Casey chairs.

Senator **Nunn**. That is what is known as SIG(I)?

General **Stilwell**. SIG(I), and they were approved there, but neither of those bodies has any authority to implement the study, direct a study, whatever, of that nature, and they were referred by Mr. Casey, therefore, to the National Security Council.

The National Security Council, advisor to the President has not acted. So while the options stand fully endorsed at the staff level, they are not yet in an operative document; therefore, they are not operative guidance for the study group to get on with the development.

Senator **Nunn**. Do all the witnesses agree with that interpretation?

Mr. **Fedor**. Certainly. I think the important thing to point out, these are study options. The study group, through these channels, is essentially recommending to the National Security Council areas that require further study by the study group.

Senator **Nunn**. Senator Glenn.

Senator **Glenn**. Thank you, Mr. Chairman. I will be brief here. Do you have any comment on the huge increase in numbers of clearances? First let me say, General, I want to associate myself with Senator Nunn's remarks earlier. I think it is important to have you willing to serve in capacities after a long and distinguished career.

The huge increase in numbers of people, I was looking at a chart from some of the testimony last week. It is a fantastic increase. We went down from 1972 to 1976; we actually had decreases in number of requests and personnel required to process those. Then it went along fairly level to about 1980; a little variation there. But then since 1980, as you can see the trend of those things, there is no end. It went from a low point in 1976 of 124,000 people being processed up to where we estimate in 1985 it will be 215,000 people. It is not quite doubled, but it is close to it in that short period of time.

What on Earth is going on? There are not that many new secret things that I know of that require that amount of increase. Are we just wild with requirements for security? Are we overdoing this because the more these numbers go up, the more difficult it becomes, the more impossible it is to really give proper screening to those who really should have access to the material.

If we make it where everybody in all of the armed services of our Nation are required to have some sort of clearance like this, we are going to make an impossible task of reviewing it.

Could you comment on that, please?

General **Stilwell**. I might add, Mr. Senator, you are dealing only there with top secret and SCI on that chart. That is not the secret.

Senator **Glenn**. This is only TS and up?

General **Stilwell**. That's correct, sir.

Senator **Glenn**. What is the figure if you include the lower classification or if you include secret in there?

Senator **Nunn**. You grossly understated the problem, Senator Glenn.

Senator **Glenn**. Not something unusual.

General **Stilwell**. You may find in my prepared statement, Mr. Senator, the DIS processed almost 900,000 requests for secret clearance.

Senator **Glenn**. You cannot process that many people in a year.

General **Stilwell**. Oh, yes, sir, you can because it is—that is one of the problems we probably should still deal with in this hearing. The requirements for secret clearance are so minimum that you can handle a lot of them because essentially it's a machine-automated exercise.

Senator **Nunn**. Agency check is what it is.

General **Stilwell**. The primary reason for the creep over these last 5 years is because of the more sensitive high-technology weapons systems and the larger, by far the largest portion of that increase is to be found in the industrial security sector. The contractor increase—I have a breakdown. In the fiscal year 1978, we investigated 27,000 contractor personnel. In the fiscal year 1984, 68,000. Now, that is at the top secret, SCI level, and our projection for this current fiscal year, which we are half way through, is 81,000, and it represents originally 19 percent of your chart, sir, of industrial security clearances, and the projection on your chart is 37. It is double the percentage.

Senator **Glenn**. In the TS category you just mentioned, it is tripling, exactly tripled, as a matter of fact, from 1978 to your estimate for 1985, from 27,000 to 81,000; that would be a tripling exactly.

General **Stilwell**. A tripling of the contractor in numbers and a doubling of the percentage of the total department because there has been some creep in the services as well.

Senator **Glenn**. Do you think our secret material is going out to too wide a group then? Everything technical did not get invented since 1978. I just cannot believe that our requirements have gone up that much. Are we too lax in spreading this too far and requiring too many people to get involved with it?

General **Stilwell**. I think it is primarily the latter. I can't gainsay the contracting officers of several services in terms of data that must be made available in their view to accomplish the development of tests, evaluation of that weapons system, but I think there is clearly erring on the side of caution, you might say it is profligate as to the number of people being cleared who really don't need to be cleared in Company A, B, or C.

Senator **Glenn**. Do you have any program to try to get contractors to hold this to a minimum? I think we are about to snow ourselves under.

General **Stilwell**. Unfortunately, Mr. Senator, the incentives have been the other way to this point.

Senator **Glenn**. They want to protect themselves, so it is easy for them—just fill out a sheet; get this guy cleared; then their skirts are cleared. They don't have to worry about them from then on because the Government has cleared them, supposedly. Is that one of the factors involved in this?

General **Stilwell**. That's correct, sir; at least in the environment that exists today in terms of responses to requests for proposals and so forth, the number of people cleared, facilities, so forth.

So that is an area we must continue to work on and very hard.

Senator GLENN. You mention in your statement about use of polygraphs, and so on, and the effectiveness of this and the Merit Systems Protection Board getting into the act on that. What is the status of that now as to validity of trying to dismiss somebody as a result of a polygraph test? Can you make it stick or do you have to find other reasons for firing him?

General STILWELL. The rules we have always operated on, sir, is indication of deception as a result of an analysis of the charts that are taken is not of itself cause for punitive action. And so it must be accompanied by other evidence that would permit you to do it.

We are doing a test, however, where there is one exception to that, sir. In the test that was authorized by the Congress and is underway right now, if an individual refuses to take a polygraph test as a condition of access to a particularly sensitive program, the head of the department, like the service secretaries, can, in fact, deny him access even if there is no other information which will substantiate the reason for that.

Senator GLENN. Let's say he takes a polygraph test and fails it in some regard. You would still have to develop other information to let that person go. The polygraph test by and of itself is not sufficient evidence to let a person go; is that correct?

General STILWELL. Correct.

Senator GLENN. Is that because of State laws or the fact polygraphs are not 100 percent or what?

General STILWELL. With respect to our program it is DOD policy. As regards State laws, I would defer to Ms. Buck on that.

Senator GLENN. Some States will not permit polygraphs?

Ms. BUCK. That is correct, sir; it does vary from State to State.

Senator GLENN. Is this where the Merit Systems Protection Board gets in? You mentioned that briefly in your statement. What has their role in this been?

General STILWELL. May I ask Ms. Buck to answer that?

Ms. BUCK. In terms of the polygraph, the polygraph issue really has not been one at stake before the Merit Systems Protection Board. They have asserted jurisdiction with respect to a number of other issues, however, involving the adjudication process, by looking at the actual reasons behind the revocation of a clearance itself.

Senator GLENN. You also mention the Army and the Air Force have their adjudication procedures all centralized and the Navy has thousands of centers, has many of them, anyway. They do not centralize theirs at all. They apparently leave it to the local command as to how they want to handle it; is that correct?

General STILWELL. They centralized their compartmented information system and adjudication process of civilian personnel. As far as the uniformed personnel, it is out at the commands.

Senator GLENN. Is that a weakness or strength, as you see it?

General STILWELL. We think that is a weakness, sir. The DOD Inspector General thinks that is a weakness. All logic suggests common standards, but we are also bucking up against a couple centuries of tradition, sir—[laughter]—and it shows——

Senator NUNN [interposing]. We run into that in some other areas.

Senator **Glenn**. Just one other question, Mr. Chairman, and then I will turn it back to you. I am interested in this huge increase in contractors and requirements for security personnel. I appreciate that. I have been in defense all my life because of my own military background, of course. It is always a problem, but this increase we go through, you state there from 27,000 to 81,000 in that short period of time, there isn't that much increased new secrecy. We have had new projects, but not of that magnitude in the classified area.

Can you give us any indication how you think we can give incentives to the contractors to really control this better rather than putting blanket requests in and just clear everybody for secret because the Government will do it anyway and protect our skirts. That is the only way I can explain that magnitude of increase that we are talking about in requests. What kind of incentives could we give the contractor to really control this thing a little bit better by their own administrative procedures? Do you have any ideas on that?

General **Stilwell**. As you inferred, sir, he gets a free ride on this because it's our Defense Investigative Service who picks up the tab for it.

Senator **Glenn**. Maybe we need to have shared expenses on this.

General **Stilwell**. His other security expenses are directly chargeable to the contract, written off as part of the contract. It may be part of our work to improve the whole acquisition process providing incentives to bring it in under estimate, under time, so forth. There has got to be a way, but I am not prepared to tell you what kind of incentive would work.

I do think we have to work in another way with our contracting officers, with our project managers, with our intelligence people, with our inspectors to ensure we minimize the access. We have a proposal that came up in the Harper Committee, sir, that merits close scrutiny, and that is to just begin terminating clearances in Company A, B, and C at the end of 5 years, for example, unless the contractor comes in with a positive request for recertification. That is one way to begin to get at this.

Senator **Glenn**. How many people do we have cleared secret and up right now—grand total? Do we have that? Not just requests per year, but grand total.

Senator **Nunn**. I think that figure is 4.2 million; isn't it?

General **Stilwell**. Within the Department itself, civilian and military, we have 2.5 million: 454,000 top secret or higher; 2 million secret; and 13,000 confidential—this last is kind of an aberration.

Senator **Nunn**. 13,000 confidential?

General **Stilwell**. It is almost a category that——

Senator **Glenn** [interposing]. That ranks along with mysterious.

Senator **Nunn**. We have one category called embarrassing.

General **Stilwell**. In industry, 128,000 at the top secret or higher level and 917,000 as secret. And then we have, of course, the Guard and Reserves who add another 400,000 to that. So the grand total then at all levels is 4 million.

Senator **Glenn**. That means 2 percent of the people in the United States, 2 out of every 100 people you walk past on the street are cleared for secret or above.

Well, I don't know how we do it, but there has to be some effort made to control the numbers in some way. That is a ridiculous figure. There are not 4 million people in the United States that need secret clearance and above.

General STILWELL. And what complicates it and what aggravates it, I should say, Mr. Senator, is that the investigative criteria for granting a secret clearance are admittedly and worrisomely very, very minimal—very, very minimal.

Senator GLENN. Thank you, Mr. Chairman.

Senator NUNN. There is an old saying, if I can recall it: a fellow says he is not worried about his wife being able to keep a secret; it's the people she tells he worries about. I am afraid we are in that situation with that many people. I guess the only comforting thought, just think if you were in the Soviet Union, General, and everything was secret. The scope of this problem does seriously tell you something about the magnitude of a totalitarian society.

General STILWELL. That is correct, sir.

Senator NUNN. The number of things we keep secret, you can multiply it by probably a thousand for what they try to keep secret. I am sure there are a lot of elements of that society, where they have so much secret, that have duplication all over the place, which we have, as you know, Senator Glenn, in some of the black programs. It is a mammoth problem.

General STILWELL. There is one other aspect of this, sir, that provides just a little bit of comfort. As we have found in other elements of security—the physical security, emission security, electronic security—that we were kind of aimlessly, mindlessly expending funds to eliminate a vulnerability without addressing whether there was an accompanying threat. So we modified a good many of our procedures, particularly in the suppression of electronic emissions so we now only do that where there is a threat.

Somehow we have got to look at our personnel security problem from the standpoint of making sure that we allocate our resources more against a threat than mere vulnerability. So one of the comforts I draw, Senator, from the great numbers of secret clearances are all those young men and women in uniform in the combat units, a lot of whom have secret clearances, but I don't think they are vulnerable. I don't think they are under threat. So that within the enormous complex of numbers, there are degrees of sensitivity, degrees of threat, and somehow we have got to better correlate all of that.

Senator NUNN. I agree. I think we may need a category that would be below the secret level that would include an awful lot of these people that really could get by with simply an agency check and realize we are just processing them. That would be a very low-threat environment.

General STILWELL. Exactly.

Senator NUNN. It seems to me we might even turn secret into that to keep the name there, but to have something between secret and top secret and move up a number of people in that secret category, hopefully not a big number, that would then get a more thorough check.

Senator GLENN. That is fine on people, but don't forget you are also dealing with specific bits of information or documents and that means you then put another requirement in here as to how you classify that information and what you put in each one of those areas people are going to be cleared for. You add complexity to the whole system. It doesn't just simplify them. It is not just people clearance, people clearance to use certain documents so you have to put them in this new category, whatever it is.

Senator **Nunn**. You are right about that. The two have to go together. Mr. Rinzel?

Mr. **Rinzel**. I just wanted to follow up on some of Senator Glenn's questions. During the course of the investigation and in the hearings, the staff has come across some suggestions that some of the Department of Defense contract projects are unnecessarily classified; that it is not simply a question of defense contractors asking for too many clearances, but that some of the projects themselves which are classified are not done so wisely or necessarily.

I have a number of questions. Who, as a practical matter, makes a decision whether a particular project is going to be classified, and is it true that there is an incentive in the Defense Department to classify projects because there are fewer hassles in competitive bidding and because there is less oversight by the Congress on those kind of contracts?

General **Stilwell**. You dealt with, it seems to me, two complete ranges; two ends of the spectrum, sir. On the higher end of the spectrum, where there might be a minimization of oversight, you are talking really special access programs which by and large are in the higher range because the criteria are that you can't have a special access program unless the normal requirement for security is judged to be inadequate and you are talking about a very small number of people. Those are the ones which my office looks at very carefully.

On the other end of the spectrum, I would ask either Mr. Snider or Mr. Fedor to supplement what I have to say, but it is, of course, not capricious. The contract you are going to let has to be dealing with equipment, components, information, technology that has already been assessed as classified well before you get into the contractual area.

Mr. **Snider**. It would be our feeling that we don't have a problem in terms of classifying contracts that shouldn't be classified.

[At this point in the hearing, Senator Glenn withdrew from the hearing room.]

[Letter of authority follows:]

U.S. SENATE,
COMMITEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITEE ON INVESTIGATIONS,
Washington, DC.

Pursuant to Rule 5 of the Rules of Procedure of the Senate Permanent Subcommittee on Investigations of the Committee of Governmental Affairs, permission is hereby granted for the Chairman, or any Member of the Subcommittee as designated by the Chairman, to conduct open and/or executive session hearings without a quorum of two Members for the administration of oaths and taking testimony in connection with hearings on "U.S. Government Personnel Security Program." These hearings are to be held on April 25, 1985.

BILL ROTH,
Chairman.
SAM NUNN,
Ranking Minority Member.

Mr. SNIDER. Decisions to classify particular contracts are normally based on classification decisions and judgments that have already been made.

We had 67,000 classified contracts let last year in the Defense Department. It is possible there may be cases, of course, in that 67,000 where we may have an overclassification problem; it is hard to say. We haven't identified that as a widespread problem, per se.

Mr. FEDOR. Additionally, the Defense Investigative Service administers the Industrial Security Program and through its representatives in the field, issues specific contract classification guidance in coordination with the project or program manager of the service sponsor. So the contractor gets specific guidance in terms of classification.

Mr. RINZEL. But at some point in the process, someone decides this particular project, whether it is before a contract is let or not, ought to be classified. Who, as a practical matter, makes that decision, and is there any review of it, or is it simply accepted?

General STILWELL. I'm not so sure we are getting to the nub of Mr. Rinzel's question here. I can only go back to the statement that it is, per se, a contract involving classified technology, equipment, information if the material that has to be sent to the contractor meets the standards of classification.

Mr. RINZEL. I understand that. But if you have a particular weapons system, an air-to-air missile, for example, that is being developed, someone decides that it is going to be classified. Who decides that and is there any review?

Mr. FEDOR. Well, the guidance for this type of decision comes out of the program manager in the Army, Navy, or Air Force. They develop classification guides; take a propeller on a submarine, for example, a certain contour of the propeller, the Navy may assign some classification to it, then the contractor is informed of that particular classification. The contractor can't determine this unilaterally.

Mr. RINZEL. What level in the Navy is that decision made at?

Mr. FEDOR. The security policy level in the Chief of Naval Operations, Office of the Director of Naval Intelligence, in coordination with the program project managers, whether it be in submarines, or whatever.

Mr. RINZEL. But I take it that it is a fairly low-level decision that is going to be accepted up the line?

Mr. FEDOR. No, sir; that is a fairly high-level decision. The guides are developed at the Director of Naval Intelligence level.

Mr. RINZEL. The guidelines, yes, but the actual decision to classify this particular project?

Mr. FEDOR. Well, then contract specifications are sent to the contractor, and the industrial security people at DIS check to see whether or not the contract guidance is being properly applied.

Mr. RINZEL. I guess we followed this as far as we are going to get.

General STILWELL. We can submit some further amplification, sir, for the record, that perhaps would get closer to your question on the whole matter of determination of classified contracts or elements of weapons production which are in the classified area.

[The information referred to follows:]

EXTRACT FROM DOD REGULATION 5200 1-R

Section 4

CLASSIFICATION GUIDES

2-400 General

a. A classification guide shall be issued for each classified system, program, plan, or project as soon as practicable before the initial funding or implementation of the system, program, plan or project. Successive operating echelons shall prescribe more detailed supplemental guides that are considered essential to assure accurate and consistent classification. In preparing classification guides, originators should review DoD 5200.1-H (reference n)).

b. Classification guides shall:

1. Identify the information elements to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly;

2. State which of the classification designations (that is, Top Secret, Secret, or Confidential) applies to each element or category of information; and

3. State declassification instructions for each element or category of information in terms of a period of time, the occurrence of an event, or a notation that the information shall not be declassified automatically without approval of the originating agency.

c. Each classification guide shall be approved personally and in writing by an official who:

1. Has program or supervisory responsibility over the information or is the senior agency official designated by the Secretary of Defense or Secretaries of the Military Departments in accordance with Section 5.3(a) of E.O. 12356 (reference (b)); and

2. Is authorized to classify information originally at the highest level of classification prescribed in the guide.

2-401 Multiservice Interest

For each classified system, program, project, plan, or item involving more than one DoD Component, a classification guide shall be issued by (a) the element in the Office of the Secretary of Defense that assumes or is expressly designated to exercise overall cognizance over it; or (b) the DoD Component that is expressly designated to serve as the executive or administrative agent for the particular effort. When there is doubt which Component has cognizance of the information involved, the matter shall be referred to the DUSD(P) for resolution.

2-402 Research, Development, Test, and Evaluation

A program security classification guide shall be developed for each system and equipment development program that involves research, development, test, and evaluation (RDT&E) of technical information. For each such program covered by an approved Decision Coordinating Paper (DCP) or Program Objective Memorandum (POM), initial basic classification guidance applicable to technical characteristics of the system or equipment shall be developed and submitted with the proposed DCP or POM to the Under Secretary of Defense for Research and Engineering for approval. A detailed classification guide shall be developed and issued as near in time as possible to the approval of the DCP or POM.

2-403 Project Phases

Whenever possible, classification guides shall cover specifically each phase of transition, that is, RDT&E, procurement, production, service use, and obsolescence, with changes in assigned classifications to reflect the changing sensitivity of the information involved.

2-404 Review of Classification Guides

a. Classification guides shall be reviewed by the originator for currency and accuracy not less than once every 2 years. Changes shall be issued promptly. If no changes are made, the originator shall so annotate the record copy and show the date of the review.

b. Classification guides issued before August 1, 1982, that are in current use must be updated to meet the requirements of paragraph 2-400 b. Such updating shall be accomplished by the next biennial review. Converting previous declassification determinations directed by classification guides shall be accomplished in accordance with the following:

1. Automatic declassification dates or events remain in force unless changed by competent authority in accordance with subsection 2-302.

2. Dates for declassification review shall be changed to automatic declassification dates or provide for the indefinite duration of classification.

2-405 Distribution of Classification Guides

a. A copy of each approved classification guide and changes thereto other than those covering SCI shall be sent to the Director of Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs), and to the Director of Information Security, ODUSD(P). A copy of each approved classification guide covering SCI shall be submitted to and maintained by the Senior Intelligence Officer who has security cognizance over the issuing activity.

b. Two copies of each approved classification guide and its changes shall be sent by the originator to the Administrator, Defense Technical Information Center (DTIC), Defense Logistics Agency, unless such guide is classified Top Secret, or covers SCI, or is determined by the approver of the guide to be too sensitive for automatic distribution to DoD Components. Each classification guide forwarded to DTIC must bear one of the following distribution limitation statements on its front cover or first page if there is no cover:

1. "U.S. Gov't and its contractors."

2. "U.S. Gov't only."

3. "DoD and DoD contractors only."

4. "DoD only."

2-406 Index of Security Classification Guides

a. All security classification guides, except as provided in subparagraph b., below, issued under this Regulation shall be listed in DoD 5200.1-I (reference (o)), on the basis of information provided on DD Form 2024, "DoD Security Classification Guide Data Elements." The originator of each guide shall execute DD Form 2024 when the guide is approved, changed, revised, reissued, or canceled, and when its biennial review is accomplished. The original copy of each executed DD Form 2024 shall be forwarded to the Director of Information Security, ODUSD(P), who will maintain the Index. Report Control Symbol DD-POL (B&AR)1418 applies to this information collection system.

b. Any classification guide that because of classification considerations is not listed in accordance with paragraph a., above, shall be reported by the originator to the Director of Information Security, ODUSD(P) The report shall include the title of the guide, its date, the classification of the guide, and identification of the originating activity. A separate classified list of such guides will be maintained. Report Control Symbol DD-POL(B&AR)1418 applies to this information collection system.

Section 5

RESOLUTION OF CONFLICTS

2-500 General

When two or more offices, headquarters, or activities disagree concerning a classification, declassification, or regrading action, the disagreement must be resolved promptly.

2-501 Procedures

If agreement cannot be reached by informal consultation, the matter shall be referred for decision to the lowest superior common to the disagreeing parties. If agreement cannot be reached at the major command (or equivalent) level, the matter shall be referred for decision to the headquarters office having overall classification management responsibilities for the Component. That office shall also be advised of any disagreement at any echelon if prompt resolution is not likely to occur.

2-502 Final Decision

Disagreements between DoD Component headquarters, if not resolved promptly, shall be referred for final resolution to the ODUSD(P).

Mr. RINZEL. I think it is relevant because of the statistics that you cited here today which are significant. There has been a large increase in contractor requests for clearances, and, it seems to me, one possibility could be the contractors are covering themselves by asking for too many clearances and another possibility is that some of the projects may be unnecessarily classified.

Senator NUNN. General Stilwell, our subcommittee has gone into three cases rather extensively—the Bell case at Hughes in previous hearings; the Harper-Schuler case at SCT; and also the Christopher Boyce case last week at TRW. In all those cases, we had very serious security breaches and extensive information was lost, that was important classified information, but in none of them can we find in any way where the contractors were held accountable for the breaches in security.

Perhaps it was not called for; perhaps investigations were made and no contractor lapses were found. In any case no fines were levied, no disciplinary action was taken; no contracts were lost. I am not sure whether anybody was fired. I think there was one transfer that was mentioned in the TRW case, the immediate supervisor of Boyce.

I have two questions, I guess. One, do you have any comments about whether in any of those cases something was appropriate and, two, is there a way to discipline contractors under the present law and regulations other than simply disqualifying them, which is a very draconian measure, particularly for contractors who are the only ones who can make a particular item of national security interest?

Is there a way to have less of a punitive measure—in other words, more options, more flexibility so you don't have to have either no punishment at all, no sanctions at all, or disqualify them completely? Do you need more flexibility in this area?

General STILWELL. We have discussed that in the past, sir. We do have essentially two methods. One is suspension for a specific period of time so they can clean up their act and demonstrate——

Senator NUNN [interposing]. If somebody is the only one who can make F-15's, C-5's or Trident submarines, that option isn't effective, is it?

General STILWELL. No.

Senator NUNN. It would be available for the small contractor out there who is easily substituted for, but not for the large primes, it seems to me. Go ahead and discuss the second one.

General STILWELL. The second one, of course, is just a flat-out termination, which I rather like, but I agree, it does come up against the problem if you only have a sole producer of something, which is something this country ought to be looking at also.

Senator NUNN. Both of those sanctions are much more likely to be applied to small contractors than large contractors. I guess my question is, don't we need a series of sanctions that can be taken against large contractors that we cannot afford to terminate or even to suspend if they are in the middle of crucial national security work?

General STILWELL. Well, it would be nice if there could be some fiscal or other penalties. I don't know what kind of a law would permit us to do that. Certainly, we can lift the clearances of individuals that were considered responsible for it. That is in itself a lesser included offense which would make it impossible for several of the company officers to continue to do business. Kathleen?

Ms. **Buck**. I would be happy to add to that. In the Defense Investigative Service, while we have some limited suspension authority, that suspension authority only is effective until the contractor corrects the deficiencies that are pointed out, which means that you could have a long period of serious deficiencies, but so long as they immediately corrected them at the time of the inspection or shortly thereafter, their clearance would be immediately reinstated.

We don't really have suspension or debarment authority as we know it on the contract side where you can actually suspend a contractor or bar a contractor for a period of time.

Senator **Nunn**. How about the appropriateness of fines, substantial monetary fines in the discretion of the executive branch to impose?

Ms. **Buck**. Unless there is fraud or a criminal penalty, we don't have anything to use like that as a deterrent.

Senator **Nunn**. Would that be advisable? Most of these cases, in terms of top level management, there is not fraud here; if anything, it is nonfeasance and perhaps in some cases malfeasance.

Ms. **Buck**. In some cases, I think they even do come fairly close to fraud. They might try to hide problems from us.

Senator **Nunn**. Do you think it would be helpful to the Department of Defense to have authority to levy fines for a range of different penalties that are basically civil in nature, not criminal?

Ms. **Buck**. Within the administration, I don't think that we have really addressed that, but in my personal opinion, I think that that might be a useful tool.

Senator **Nunn**. Would you all think about that, and if you have further thoughts on it, supply it to us, either for the record in any form, whichever you prefer.

General **Stilwell**. We are in an area now, Mr. Chairman, that seems to me involve linkage which has never been adequately strong between security, on the one hand, and management and command, on the other. Because it seems to me the type of actions we are talking about, although it is precipitated by security violations, is one that ought to be looked at by command or the managers that make the decisions.

Debarment, which is another sanction—one answer is debarment, which has nothing to do with security, per se, but permits, doesn't qualify them to bid on the next range of contracts.

Senator **Nunn**. That is a very good, strong sanction and I think very effective at the small and medium level of business, but where there are only two or three competitors, for instance, shipyards, aircraft carriers or submarines, there are two or three people bidding and the Government says to one of them, "We are going to punish them by no longer letting you bid, you have lax security, gross negligence," what you have done is shutout the competition and ensured, in effect, that the taxpayers are going to pay a lot more for the particular ship being built or plane being built.

So that kind of sanction is kind of like capital punishment for running a red light. I do not think it has all that much credibility in terms of the major contractors. For a small, medium business, I think it can be devastating, and I am sure it is a very effective threat for them.

We need to think about that. Let me ask a couple more questions. We have heard testimony about the difficulty of obtaining law enforcement records from State, sometimes local jurisdictions. Have you run into that a great deal and, if so, is there anything that can be done about that, as you suggest, of, let's say, a legislative or regulatory nature?

General **Stilwell**. It is a substantial problem for the Defense Investigative Service, sir, and it sometimes results in the issuance of a clearance while realizing that there may be something out there in the public domain that would condition and result in a nonclearance.

So we have had two basic types of problems. One is the refusal of State authorities to recognize the decision of the Attorney General that this DIS is, in fact, a law enforcement agency and not provide information regarding criminal history. The other is some jurisdictions cannot handle our requests without payment on our part. The latter being the lesser in our view of the two evils, except it runs us against the basic principle within the Department of Defense that we don't pay for criminal history record checks required for personnel security investigations.

Mr. O'Brien, as I think he may have mentioned in his testimony, sir, and his people are working with the State jurisdictions to try to do something about it, particularly as to access. It is a mixed bag across the country today. Our concern is an increase in denial. So if there were some way in which there could be a legislative action that would be binding on State authorities, we would really welcome that.

Senator **Nunn**. We are going to look into that.

Mr. **Fedor**. Senator Nunn, in 1982, Congress passed Public Law 97-252 which was part of the Defense authorization bill, I believe, for that year. However, it really did not go far enough. It simply pointed out that the Defense Investigative Service is authorized to request information on individuals who are being investigated for recruitment and only mentions access to classified information in terms of personnel, being enlisted in the armed services. This does not cover our greater need in industry and of civilian employees with respect to personnel security investigations.

[Information submitted subsequent to the hearing follows:]

50 U.S.C.

CHAPTER 37, CRIMINAL HISTORY RECORD INFORMATION FOR NATIONAL SECURITY PURPOSES

SECTION 1901. DEFINITION.

As used in this chapter:

(a) "Criminal justice agency" includes federal, state and local agencies and means: (1) courts or (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(b) "Criminal history record information" means: information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correction supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

(c) "Classified information" means information or material designated pursuant to the provisions of a statute or Executive Order as requiring protection against unauthorized disclosure for reasons of national security.

(d) "State" means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, Guam, the Virgin Islands, American Samoa, the Trust Territory of Pacific Islands, and any other territory or possession of the United States.

(e) "Local" and "locality" mean any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal or other local government level.

SECTION 1902. RELEASE OF CRIMINAL HISTORY RECORD INFORMATION.

Upon request by the Department of Defense, criminal justice agencies shall make available criminal history record information regarding individuals under investigation by the Department of Defense for the purpose of determining eligibility for (1) access to classified information, (2) assignment to or retention in sensitive national security duties, or (3) acceptance or retention in the armed services. Fees charged for providing criminal history record information pursuant to this section shall not exceed those charged to criminal justice agencies for such information.

SECTION 1903. CONSENT REQUIRED.

The Department of Defense shall not obtain criminal history record information pursuant to this section unless it has received written consent from the individual under investigation for the release of such information for one or more of the purposes set forth in section 1902.

SECTION 1904. DISCLOSURE LIMITATIONS.

Criminal history record information received under this section shall not be disclosed except for the purposes set forth in section 1902 or as provided by the Privacy Act, 5 U.S.C.§552a.

SECTION 1905. EFFECT ON OTHER LAWS.

Section 1902 shall apply notwithstanding any other provision of law or regulation of any State or of any locality within a State, or any other law of the United States. Section 520a of Title 10 of the United States Code is hereby repealed.

SECTION 1906. EFFECTIVE DATE.

This Act shall become effective with respect to any inquiry conducted by the Department of Defense for any of the purposes specified in section 1902 which begins after the date of enactment of this Act.

Senator NUNN. Did it take care of the ones in the armed services?

Mr. FEDOR. It did not. I am not a lawyer, but I understand there may be a constitutional problem here. It authorized the designated defense investigative agency to solicit the information, but it did not, of course, put any pressure on the States to release the information, and this is a problem. For example, it had no effect on the State of California with respect with its labor code which prohibits the use of criminal history record information for "employment purposes" and the California authorities told us issuance of security clearances by the Department of Defense, whether it be to industrial employees, military, or DOD civilians, in their mind is an employment purpose.

Senator NUNN. Mrs. Buck, if you have an administration position on that that is forthcoming, we would like to have it. But in the absence of that, if you could give us your personal expert opinion on what our options might be legally in this area, things you believe to be constitutional, then we could ask for the administration's reaction to those at a later point. You don't want to go through the whole approval process and wait for 8 months and a year to see where it turns out.

If you give us some options to consider—you don't have to express a preference—what we could consider in this area.

Ms. BUCK. On this particular question, a very straightforward legislative proposal could be developed that has no constitutional problems. Over the last 20 years, some of the States have passed privacy laws or labor laws which within those States would preclude the local law enforcement agencies from providing arrest records where there was no conviction.

When our Defense Investigative Service agent goes in to try to obtain the information, the local law enforcement people say they can't provide that because of this particular State law. We have taken the legal position that under the supremacy clause we should be able to obtain that information for national security purposes, that you need to distinguish between employment and national security reasons.

In many jurisdictions, the States have concurred in that legal interpretation. In some States, there is still some confusion, especially when you get down to your local, very small police force. They don't understand the legal niceties of the situation; it is difficult. I think a statute along the lines of what we have been talking about here that made it clear access for national security purposes, not employment, must be provided to solve the problem.

Senator NUNN. Not for employment purposes.

Ms. BUCK. That would take care of it; yes.

Senator NUNN. Could you furnish us such a rough draft?

Ms. BUCK. I am sure we could. We will be happy to work with you and your staff on that.

Senator NUNN. Good. You were going to add something else. I didn't mean to interrupt.

Ms. BUCK. I think this discussion highlights the confusion between employment and security clearances. In our judgment, there is clearly a distinction. This raises the issue of the Merit Systems Protection Board. In my prepared testimony which you have in the record, I explain this issue at length. But just to state it briefly, the Merit Systems Protection Board, I think, is erroneously concluding they have jurisdiction under their specific provisions regarding disciplinary action against employees to get into the security clearance process itself and examine the reasoning of the agency and criterion used by the agency in either denying or granting clearances.

I think this is another area that poses serious problems for us where legislation could be helpful.

Senator NUNN. Can they, in effect, overrule a security determination now?

Ms. BUCK. Yes; that is correct. They have done that in a number of cases. We have filed an amicus brief before the Merit Systems Protection Board on this issue, as has the Office of Personnel Management.

Senator NUNN. That is still pending?

Ms. BUCK. That is still pending; yes.

Senator NUNN. I guess that gets back to the problem we have with the number of people involved here, too.

Ms. **Buck**. It is not only with the numbers, but when you believe you have information which is derogatory and the person should not be granted a clearance or the clearance revoked, it is a problem in which you have other entities which ordinarily would not deal with national security problems second guessing the agents on the actual factual decisions which were made.

Senator **Nunn**. Can you draw a line between employment criterion and national security criterion? For instance, if a report comes in from DIS that an individual has very extensive problems with alcohol. If you are going through the adjudication on national security, that rings a bell, but if you are also going through the question of whether the individual should be hired or not, it seems to me that is relevant to both of those inquiries. So how do you draw, or is there a way to draw the line?

Ms. **Buck**. Some facts which come up in the adjudiciation process may be relevant for suitability and security purposes. Alcoholism might not only be a relevant factor in determining whether a person is suitable, but also a relevant factor to determine whether that person should be granted access to classified information. There is a case I think you can make on that that it is relevant for both purposes. We have a special statute, the Rehabilitation Act that deals with Federal employment on that issue and that has been a particular problem that has been raised in some of the MSPB cases involving alcohol abuse.

In those cases the Federal employee argued the Agency may not be able to terminate employment for that purpose, but does that mean that we would have to entrust that person who is an admitted alcoholic with the secrets of our Nation?

Senator **Nunn**. Should not; no.

Ms. **Buck**. We have contended, no, there is clearly a distinction which should be made there.

Senator **Nunn**. I agree with you on that. I have a number of other questions, but let me just ask my final question here, and I will submit the rest for the record, and I will also announce the record will be open for about 2 weeks here, so that we can add any supplements any of our witnesses choose to add.

The Harper report had an extensive number of recommendations; a good number of them, maybe half had something to do with personnel security.

What is the status of this report now and the status of the implementation? Are you implementing a number of those recommendations?

General **Stilwell**. A short answer to that, Mr. Chairman, is yes. There were some 39 recommendations that were prepared by that very fine committee which I chartered in the wake of that episode on the west coast. Our own analysis is that about 28 of the 39 should be implemented, either implemented immediately or taken under further advisement for modification.

There are two categories where we backed away from. One were those which were so resource intensive that we accepted them as an ideal to work toward but couldn't do anything about it now and the other where we disagreed in principle, for example, those which would have put DIS people in sort of an adversarial position, vis-a-vis the industrial concerns or the question of separate hotline, and so forth.

By and large, we felt it was a very excellent product that merits implementation in part and further elaboration with a view to longer-range implementation. I can give you—I think your committee may have it, sir.

Senator **NUNN**. I have read a large portion of it myself. We have summaries of it, too. It has been very helpful to us in these hearings. This is, I think, a very well-done document, and we will be reviewing it again carefully in making our own recommendations.

Do any of you have any other things you would like to recommend to us from a legislative point of view? Any other points you would like to make this morning?

General **STILWELL**. I guess the only basic summation I would make, sir, is, again, to underscore our applause for the initiative that this subcommittee has taken and to underscore that we are dealing with an area which demands the level best efforts of all people in the executive branch, in the Congress to the end that we can produce a coherent, cost-effective complete security system that is consistent with the imperatives of national security.

Senator **NUNN**. Thank you very much, General. Do any of you other witnesses have any?

Mr. **FEDOR**. I would just like to add, Senator Nunn, I believe the record of this hearing, as comprehensive and wide-ranging as it is, will be of great value to the NSDD-84 study group when they reconvene.

Senator **NUNN**. I am glad to hear that. We appreciate it very much. Do you have anything?

Ms. **BUCK**. No, sir.

Senator **NUNN**. Mr. Snider.

Mr. **SNIDER**. No, sir.

Senator **NUNN**. Thank you all for being here.

[The prepared statements of General Stilwell and Ms. Buck, with attachments, follow. Responses to written questions from General Stilwell and Ms. Buck also follow:]

PREPARED STATEMENT OF GEN. RICHARD G. STILWELL

MR. CHAIRMAN, I APPRECIATE THE OPPORTUNITY TO APPEAR BEFORE THE SUBCOMMITTEE TODAY TO PRESENT AN OVERVIEW OF THE DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM AND TO DISCUSS SUCH SPECIFIC PERSONNEL SECURITY POLICY MATTERS AS YOU MAY WISH.

TRADITIONALLY, THERE HAS BEEN A THREE-PRONGED APPROACH TO PROVIDING SECURITY TO SENSITIVE GOVERNMENT PROGRAMS: INFORMATION SECURITY, PHYSICAL SECURITY, AND PERSONNEL SECURITY.

HISTORICALLY, THE GOAL OF PERSONNEL SECURITY HAS BEEN TO ASCERTAIN THE TRUSTWORTHINESS OF INDIVIDUALS PRIOR TO THEIR BEING GRANTED ACCESS TO CLASSIFIED INFORMATION OR PRIOR TO THEIR BEING ASSIGNED TO SENSITIVE NATIONAL SECURITY DUTIES--AND THEIR CONTINUING TRUSTWORTHINESS AFTERWARDS. WE DO NOT TAKE THIS RESPONSIBILITY LIGHTLY--FOR WE ARE AWARE THAT BOTH INDIVIDUAL AND NATIONAL SECURITY INTERESTS ARE INVOLVED. PEOPLE ARE CENTRAL TO THE SECURITY ISSUE. ONE CAN INSTALL THE MOST COMPREHENSIVE AND SOPHISTICATED PHYSICAL AND INFORMATION SECURITY CONTROLS IMAGINABLE, YET THEY WILL NOT PREVENT A CLEARED EMPLOYEE FROM COMPROMISING OUR SECRETS IF HE CHOOSES TO BREAK THE TRUST THAT HIS GOVERNMENT HAS AFFORDED HIM.

THE ULTIMATE THRUST OF PERSONNEL SECURITY, THEREFORE, IS TO IDENTIFY PERSONS WHO MAY NOT BE RELIED UPON TO PROTECT LEGITIMATE NATIONAL SECURITY SECRETS BEFORE THEY ARE GIVEN ACCESS AND, OF GREATER IMPORTANCE, TO INSURE THAT THOSE ALREADY GIVEN ACCESS ARE PERSONALLY DISPOSED TO CONTINUE TO

MEET THEIR OBLIGATIONS TO SAFEGUARD SUCH INFORMATION.

THE KEYSTONE TO PERSONNEL SECURITY IN THE DEFENSE DEPARTMENT, AS IN MOST GOVERNMENT AGENCIES, HAS LONG BEEN THE PERSONNEL SECURITY FIELD INVESTIGATION, OR BACKGROUND INVESTIGATION, CONSISTING OF CHECKS WITH NATIONAL AND LOCAL LAW ENFORCEMENT AGENCIES, EMPLOYMENT AND CREDIT REFERENCES, AND INTERVIEWS WITH FRIENDS, NEIGHBORS, CO-WORKERS, AND OTHERS WHO ARE IN A POSITION TO COMMENT ON THE INDIVIDUAL'S RELIABILITY AND TRUSTWORTHINESS. RARELY DO THESE CHECKS DISCLOSE EVIDENCE OF COVERT CONTACTS OR ATTEMPTED PENETRATIONS BY FOREIGN INTELLIGENCE. RATHER THEIR VALUE LIES IN UNCOVERING PERSONAL CONDUCT INFORMATION THAT MAY REFLECT POTENTIAL VULNERABILITY TO HOSTILE APPROACHES AND, MORE OFTEN, DEVELOP INFORMATION INDICATING THAT THE SUBJECT'S PERSONAL TRAITS ARE SUCH THAT HE OR SHE SIMPLY COULD NOT BE RELIED UPON TO SAFEGUARD NATIONAL SECURITY INFORMATION.

WE HAVE PROVIDED THE SUBCOMMITTEE WITH COPIES OF OUR PERSONNEL SECURITY POLICY DOCUMENTS DETAILING THE DOD PROGRAMS IN THE PERSONNEL SECURITY AREA. ADDITIONALLY, THE DIRECTOR OF THE DEFENSE INVESTIGATIVE SERVICE IN HIS PRESENTATION BEFORE THE SUBCOMMITTEE HAS COVERED THE ROLE OF THE DEFENSE INVESTIGATIVE SERVICE IN IMPLEMENTING THIS PROGRAM. I WILL NOT REPEAT THOSE DETAILS HERE.

I DO WANT, HOWEVER, TO HIGHLIGHT THE KEY FEATURES OF THE DEFENSE PROGRAM AS WELL AS MENTION SEVERAL ONGOING EFFORTS BOTH IN DOD AND WITH THE EXECUTIVE BRANCH WHICH WILL UNDOUBTEDLY HAVE A SIGNIFICANT IMPACT UPON THE DOD PROGRAM.

THE FIRST CRUCIAL POINT TO EMPHASIZE IS ITS SCOPE. THE DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM IS BY FAR THE LARGEST IN THE FEDERAL GOVERNMENT. INDEED, THERE ARE MORE PEOPLE CLEARED UNDER THE DEFENSE PROGRAM THAN IN THE REST OF THE FEDERAL GOVERNMENT. THE GENERAL ACCOUNTING OFFICE REPORTS THAT OVER 90% OF THE SENSITIVE POSITIONS IN THE FEDERAL GOVERNMENT ARE IN THE DEPARTMENT OF DEFENSE. THERE ARE 2.5 MILLION CLEARED DOD MILITARY/CIVILIAN EMPLOYEES, 1.4 MILLION CLEARED INDUSTRIAL EMPLOYEES AND APPROXIMATELY 400,000 CLEARED MEMBERS OF THE NATIONAL GUARD AND RESERVE FORCES. THESE FIGURES INCLUDE INDIVIDUALS CLEARED FOR 105 SPECIAL ACCESS PROGRAMS INVOLVING INFORMATION OF THE HIGHEST NATIONAL SECURITY SENSITIVITY.

CONDUCTING TIMELY AND PRODUCTIVE INVESTIGATIONS AT THIS VOLUME, ADJUDICATING THE RESULTS OF THE CASES COMPLETED, AND, AFTERWARDS, MAINTAINING SECURITY SUPERVISION OF THESE VAST NUMBERS OF CLEARED INDIVIDUALS ARE FORMIDABLE TASKS, BOTH IN TERMS OF ADJUSTING POLICY AND RESOURCES TO MEET THE DEPARTMENT'S OPERATIONAL REQUIREMENTS, AND TO ENSURE BASIC FAIRNESS TO THOSE WHO ARE SUBJECT TO THIS PROCESS.

POLICY DEVELOPMENT IS CENTRALIZED AT DOD LEVEL WITHIN DUSD(P). THE DEFENSE INVESTIGATIVE SERVICE HAS SOLE RESPONSIBILITY TO CARRY OUT BACKGROUND INVESTIGATIONS OF ALL DEFENSE EMPLOYEES AND CONTRACTORS. HOWEVER, IMPLEMENTATION OF POLICY IS DECENTRALIZED AT DOD COMPONENT LEVEL. IT IS ULTIMATELY THE RESPONSIBILITY OF THE SECRETARIES OF THE MILITARY DEPARTMENTS, AND THE HEADS OF THE DEFENSE AGENCIES, HOWEVER, TO INSURE THAT PERSONS ACCEPTED FOR OR RETAINED IN THE ARMED FORCES, PERSONS SELECTED FOR OR ASSIGNED TO SENSITIVE CIVILIAN POSITIONS, AND PERSONS AFFORDED ACCESS TO CLASSIFIED INFORMATION, INCLUDING THOSE EMPLOYED UNDER NATIONAL SECURITY CONTRACTS, ARE RELIABLE AND TRUSTWORTHY. THE LEGAL BASES FOR THE DOD PERSONNEL SECURITY PROGRAM ARE FOUND IN EXECUTIVE ORDER 10450 WHICH GOVERNS THE CIVILIAN PROGRAM, EXECUTIVE ORDER 10865 WHICH GOVERNS THE INDUSTRIAL PROGRAM, AND EXECUTIVE ORDER 12356 WHICH GOVERNS ACCESS TO NATIONAL SECURITY INFORMATION. WHILE THERE IS NO EXECUTIVE ORDER EXPLICITLY ADDRESSING MILITARY PERSONNEL SECURITY, OUR AUTHORITY IN THIS AREA DERIVES FROM THE NATIONAL SECURITY ACT OF 1947 WHICH PROVIDES THE SECRETARY OF DEFENSE WITH GENERAL AUTHORITY TO OPERATE THE DEPARTMENT IN AN EFFECTIVE, EFFICIENT MANNER.

INVESTIGATIONS AND SECURITY SUPERVISION

THE DEPARTMENT CONDUCTS A VARIETY OF BACKGROUND INVESTIGATIONS, DEPENDING UPON THE LEVEL OF ACCESS NEEDED BY THE INDIVIDUAL CONCERNED. THESE ARE DETAILED IN THE STATEMENT PROVIDED BY THE DIRECTOR OF THE DEFENSE INVESTIGATIVE SERVICE, HOWEVER, SO I NEED NOT REPEAT THEM. SUFFICE IT TO SAY, THE PROCESS BY WHICH WE ARRIVE AT THE INVESTIGATIVE SCOPE FOR A PARTICULAR TYPE OF INVESTIGATION HAS BEEN A DYNAMIC ONE WITHIN DEFENSE. THIS IS NECESSITATED BY THE FACT THAT WE HAVE EXTREMELY LIMITED RESOURCES TO CONDUCT THE VAST NUMBERS OF INVESTIGATIONS THAT ARE REQUESTED TO CARRY OUT THE DEFENSE MISSION. SO IT IS NOT SIMPLY A MATTER OF SELECTING CERTAIN

ELEMENTS OF AN INVESTIGATION FOR VARYING LEVELS OF CLEARANCE. RATHER, THE POTENTIAL OF EACH INVESTIGATIVE ELEMENT TO PRODUCE INFORMATION ESSENTIAL TO A TRUSTWORTHINESS DETERMINATION MUST BE WEIGHED AGAINST THE INVESTIGATIVE RESOURCES AVAILABLE. SINCE THOSE RESOURCES ARE SCARCE, WE SEARCH FOR TECHNIQUES THAT WILL PROVIDE US WITH THE MOST PRODUCTIVE INFORMATION WITH THE LEAST AMOUNT OF INVESTIGATIVE EFFORT.

AN EXAMPLE OF THIS PROCESS IS THE RELATIVELY NEW INTERVIEW-ORIENTED BACKGROUND INVESTIGATION, OR IBI, MENTIONED BY MR. O'BRIEN. UNDER A TEST OF THIS CONCEPT IN 1981, WE FOUND THAT SIMPLY BY DIRECT AND IN-DEPTH QUESTIONING OF THE SUBJECT, WE WERE ABLE TO DEVELOP ALMOST THREE TIMES THE AMOUNT OF DEROGATORY INFORMATION PREVIOUSLY BEING DEVELOPED BY INVESTIGATIONS THAT DID NOT INCLUDE A SUBJECT INTERVIEW. ALTHOUGH THESE INTERVIEWS THEMSELVES ARE TIME-CONSUMING AND AT THE TIME THEY WERE PUT IN PLACE FORCED US TO CUT BACK TEMPORARILY ON OTHER ELEMENTS OF THE INVESTIGATION, WE FOUND THEM JUSTIFIED IN TERMS OF THE RELATIVELY HIGH RATE OF PRODUCTIVITY.

WE NOW HAVE HAD FOUR SUCCESSFUL YEARS OF EXPERIENCE WITH THE IBI AND OUR CUSTOMERS SEEM PLEASED WITH IT. ELEMENTS OF THE INVESTIGATION WHICH WERE TEMPORARILY SUSPENDED IN 1981 HAVE NOW BEEN ADDED BACK TO THE SCOPE, AND WE FIND THAT THE RESULTANT COMBINATION IS MORE PRODUCTIVE OF ADVERSE INFORMATION THAN THE SPECIAL BACKGROUND INVESTIGATION REQUIRED FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION.

ALTHOUGH WE DEPEND HEAVILY UPON THE PERSONNEL SECURITY

INVESTIGATIVE PROCESS AS THE INITIAL BASIS FOR A CLEARANCE, WE HAVE LONG RECOGNIZED THAT IT WOULD BE UNWISE TO RELY EXCLUSIVELY ON PERSONNEL SECURITY INVESTIGATIONS AS THE SOLE MEANS OF ASSURING THE CONTINUED SECURITY TRUSTWORTHINESS OF INDIVIDUALS. INDEED, THE EFFECTIVENESS OF THE GOVERNMENT INVESTIGATIVE PROCESS, GENERALLY, AND THE AVAILABILITY AND UTILITY OF SOURCES OF INFORMATION, PARTICULARLY, HAS ERODED OVER THE YEARS. SIMPLY STATED, A PERSONNEL SECURITY INVESTIGATION IS NOT AS PRODUCTIVE OF RELEVANT ADJUDICATIVE INFORMATION AS IT WAS 20 YEARS AGO. THIS CAN BE ATTRIBUTED TO A NUMBER OF FACTORS, AMONG THEM THE PRIVACY ACT OF 1974, THE FAMILY EDUCATION AND RIGHT TO PRIVACY RECORDS ACT OF THE SAME YEAR, THE INCREASING RELUCTANCE OR INABILITY OF STATE AND LOCAL JURISDICTIONS TO PROVIDE CRIMINAL HISTORY RECORD INFORMATION, THE HIGH MOBILITY OF OUR CITIZENS WHICH MAKES RESIDENCE CHECKS LESS USEFUL, AND A GROWING RELUCTANCE ON THE PART OF OUR CITIZENS, IN GENERAL, TO PROVIDE THE KIND OF PERSONAL INFORMATION WHICH MAY IMPACT ON CLEARANCES AND CAREERS.

CONSEQUENTLY, TO SUPPLEMENT THE INVESTIGATIVE PROCESS, THE DOD PROGRAM EMPHASIZES CONTINUING SECURITY EVALUATION OF PERSONS ALREADY CLEARED AND FUNCTIONING IN SENSITIVE POSITIONS. THE RESPONSIBILITY FOR SUCH ASSESSMENT IS SHARED BY THE ORGANIZATIONAL COMMANDER OR MANAGER, THE INDIVIDUAL'S SUPERVISOR AND, IN A LARGE MEASURE, THE INDIVIDUAL HIMSELF. TO THIS END, THE HEADS OF DOD COMPONENTS MAINTAIN PROGRAMS DESIGNED TO EVALUATE ON A CONTINUING BASIS THE STATUS OF PERSONNEL

UNDER THEIR JURISDICATION WITH RESPECT TO SECURITY ELIGIBILITY. THESE PROGRAMS REQUIRE CLOSE COORDINATION BETWEEN DOD SECURITY AUTHORITIES AND PERSONNEL, MEDICAL, LEGAL AND SUPERVISORY OFFICIALS TO ASSURE THAT ALL PERTINENT INFORMATION AVAILABLE WITHIN AN ORGANIZATION IS CONSIDERED IN THE PERSONNEL SECURITY EVALUATIVE PROCESS. THESE PROGRAMS WORK. INDEED, THE OVERWHELMING MAJORITY OF SUSPENSIONS OR REVOCATIONS OF CLEARANCES IS BASED ON ADVERSE INFORMATION DEVELOPED WITHIN THE ORGANIZATIONAL MANAGEMENT SYSTEM RATHER THAN THROUGH THE NORMAL INVESTIGATIVE PROCESS.

SIMILARLY, UNDER THE DEFENSE INDUSTRIAL SECURITY PROGRAM WHICH IS MANAGED BY DOD FOR 18 OTHER FEDERAL AGENCIES, CONTRACTORS ARE REQUIRED TO REPORT TO THE DEPARTMENT OF DEFENSE DEROGATORY INFORMATION WHICH COULD ADVERSELY EFFECT A CONTRACTOR EMPLOYEE'S CLEARANCE. THIS, TOO, CONSTITUTES AN IMPORTANT FEATURE OF THE INDUSTRIAL PROGRAM.

IN ADDITION TO INVESTIGATING REPORTS OF DEROGATORY INFORMATION INVOLVING CLEARED PERSONNEL, DOD ALSO CONDUCTS PERIODIC REINVESTIGATIONS OF PERSONS ACCESSING SENSITIVE COMPARTMENTED INFORMATION, HOLDING TOP SECRET CLEARANCE, OR ASSIGNED TO CERTAIN ESPECIALLY SENSITIVE POSITIONS. THE PERIODIC REINVESTIGATION (PR) SCOPE UTILIZED BY DOD IS THE MOST COMPREHENSIVE IN THE FEDERAL GOVERNMENT. HOWEVER, BECAUSE OF RESOURCE LIMITATIONS, WE HAVE FOUND IT NECESSARY TO LIMIT THE NUMBER OF PERIODIC REINVESTIGATIONS BY ASSIGNING QUOTAS TO THE REQUESTING AGENCIES--WITH A CURRENT ANNUAL CEILING OF 40,000. WHILE WE WOULD LIKE TO COVER ALL PERSONS

WITH TOP SECRET CLEARANCES AT FIVE-YEAR INTERVALS, THE PERSONS NOW REQUIRING SUCH PERIODIC REINVESTIGATION ARE ESTIMATED AT 279,000 PERSONS, WITH AN ESTIMATED 296,000 ADDITIONAL JOINING THE LIST BETWEEN 1985-1988. THE DEFENSE INVESTIGATIVE SERVICE WOULD HAVE TO AVERAGE 115,000 PRs ANNUALLY, NECESSITATING AN AUGMENTATION OF DIS BY 767 INVESTIGATIVE PERSONNEL. WERE THE PERIODIC REINVESTIGATION APPLIED TO PERSONS CLEARED AT THE SECRET LEVEL, THREE MILLION ADDITIONAL PERSONS WOULD REQUIRE REINVESTIGATION--AND AN ADDITIONAL DIS AUGMENTATION OF 4841 INVESTIGATIVE PERSONNEL PLUS THE NECESSARY AUXILIARY SUPPORT.

IN SHORT, BECAUSE OF THESE RESOURCE LIMITATIONS, WE HAVE HAD TO FOCUS OUR REINVESTIGATIONS UPON THOSE WITH ACCESS TO THE MOST SENSITIVE CLASSIFIED INFORMATION. IN THIS CONNECTION, OUR GREATEST PERSONNEL SECURITY CONCERN INVOLVES THOSE PERSONS WHO HAVE BEEN CLEARED FOR, AND WHO HAVE HAD ACCESS FOR A PERIOD OF TIME TO, SO-CALLED "SPECIAL ACCESS PROGRAMS". BY DEFINITION UNDER EXECUTIVE ORDER 12356 A SPECIAL ACCESS PROGRAM MAY BE CREATED ONLY IF (1) NORMAL MANAGEMENT AND SAFEGUARDING PROCEDURES DO NOT LIMIT ACCESS SUFFICIENTLY; AND (2) THE NUMBER OF PERSONS WITH ACCESS IS LIMITED TO THE MINIMUM NECESSARY TO MEET THE OBJECTIVE OF PROVIDING EXTRA PROTECTION FOR THE INFORMATION. IN DOD, SPECIAL ACCESS PROGRAMS PROTECT BASICALLY INTELLIGENCE, RESEARCH AND DEVELOPMENT, AND SPECIAL MILITARY ACTIVITIES. WE ARE PARTICULARLY CONCERNED WITH PROVIDING SUFFICIENT PROTECTION TO THESE PROGRAMS.

USE OF THE POLYGRAPH TO SUPPLEMENT INVESTIGATIONS

IN NOVEMBER 1981, SOON AFTER TAKING RESPONSIBILITY FOR THIS PROGRAM, I COMMISSIONED A SELECT PANEL, COMPOSED OF SENIOR DEFENSE OFFICIALS, AND CHARGED THEM WITH REVIEWING THE DOD PERSONNEL SECURITY PROGRAM FROM TOP TO BOTTOM AND DEVELOPING RECOMMENDATIONS FOR IMPROVEMENT OF THE EXISTING SYSTEM. THE PANEL WAS CHAIRED BY THE DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR ADMINISTRATION, AND CONSISTED OF THE NAVY GENERAL COUNSEL; THE DIRECTOR OF THE ARMY STAFF; THE DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE FOR LOGISTICS; THE DEPUTY DIRECTOR, NSA; AND THE CHIEF OF STAFF, DIA.

THE PANEL CONDUCTED A COMPREHENSIVE REVIEW AND ISSUED A LENGTHY REPORT IN APRIL 1982, RECOMMENDING A NUMBER OF ACTIONS TO ENHANCE THE PERSONNEL SECURITY PROGRAM (AND I AM PLEASED TO REPORT WE HAVE TAKEN ACTION ON VIRTUALLY ALL OF THEM). OF PARTICULAR INTEREST WITH RESPECT TO SPECIAL ACCESS PROGRAMS, WAS THE PANEL'S RECOMMENDATION THAT A LIMITED, COUNTERINTELLIGENCE-SCOPE POLYGRAPH BE CONSIDERED TO ASSIST IN DETERMINING THE INITIAL AND CONTINUED ELIGIBILITY OF A FINITE NUMBER OF INDIVIDUALS TO POSITIONS INVOLVING ACCESS TO EXTREMELY SENSITIVE CLASSIFIED INFORMATION. COUNTERINTELLIGENCE QUESTIONS WOULD BE LIMITED TO QUESTIONS SUCH AS: HAVE YOU EVER ENGAGED IN ESPIONAGE OR SABOTAGE AGAINST THE UNITED STATES?; DO YOU KNOW ANYONE WHO IS ENGAGED IN ESPIONAGE OR SABOTAGE OF THE UNITED STATES?

THIS RECOMMENDATION WAS SUBSEQUENTLY INCORPORATED INTO A PROPOSED REVISION OF THE DEPARTMENT'S POLYGRAPH DIRECTIVE

WHICH WAS ALREADY IN THE WORKS. AFTER ALMOST TWO YEARS OF CONSIDERATION, WHICH INCLUDED TWO ROUNDS OF COORDINATION INTERNALLY AND REPEATED DISCUSSIONS WITH THE PUBLIC AND WITH CONGRESSIONAL STAFFS, LAST YEAR THE CONGRESS APPROVED A LIMITED TEST OF THIS APPROACH DURING THIS FISCAL YEAR.

WE BELIEVE--ON THE BASIS OF OUR EXTENSIVE EXPERIENCE WITH THE POLYGRAPH--THAT THIS UNIQUE INVESTIGATIVE TOOL CAN, WHEN PROPERLY CONTROLLED, BE EMPLOYED IN A MANNER THAT DOES NOT VIOLATE THE RIGHTS AND PRIVACY OF OUR EMPLOYEES, AND YET PROVIDE THE DEPARTMENT WITH A GREATER DEGREE OF SECURITY ASSURANCE WITH RESPECT TO OUR MOST SENSITIVE PROGRAMS, THAN WE NOW HAVE. WE BELIEVE THE MERE POSSIBILITY OF BEING SUBJECTED TO A POLYGRAPH EXAMINATION WILL ACT AS A POWERFUL DETERRENT TO THOSE INDIVIDUALS WHO MIGHT CONSIDER AN ATTEMPT TO PENETRATE OR COMPROMISE SUCH PROGRAMS. RECENT HISTORY CLEARLY INDICATES THE EXTENT OF DAMAGE THAT CAN BE CAUSED BY EVEN ONE PERSON WHO HAS ACCESS TO SENSITIVE INFORMATION WHO IS WILLING TO SHARE THAT INFORMATION WITH OUR ADVERSARIES.

ACCEPTANCE OF PRIOR SECURITY CLEARANCE DETERMINATIONS

DOD POLICY ALSO STRESSES AVOIDANCE OF UNNECESSARY OR DUPLICATIVE INVESTIGATIONS. WITHIN DEFENSE, SECURITY CLEARANCES ARE MUTUALLY AND RECIPROCALLY ACCEPTABLE SO LONG AS THERE HAS BEEN NO BREAK IN FEDERAL SERVICE GREATER THAN 12 MONTHS AND NO DEROGATORY INFORMATION IS KNOWN THAT MAY HAVE OCCURRED SUBSEQUENT TO THE LAST SECURITY DETERMINATION. CONSIDERING THE LARGE NUMBER OF CLEARED DOD PERSONNEL WHO MOVE TO NEW

ASSIGNMENTS EACH YEAR THIS ELIMINATES UNNECESSARY DUPLICATION AND A COSTLY ADMINISTRATIVE BURDEN. THE POLICY ALSO APPLIES TO THE CONTRACTOR ARENA WHEREIN A CLEARED EMPLOYEE AT ONE FIRM MAY TRANSFER TO ANOTHER, WITH DIS TRANSFERRING THE SECURITY CLEARANCE WITHOUT DELAY. PRIOR INVESTIGATIONS CONDUCTED BY DOD OR ANOTHER FEDERAL AGENCY ARE ACCEPTED SO LONG AS THERE IS NO BREAK IN EMPLOYMENT GREATER THAN 12 MONTHS AND THE INVESTIGATION IS OF SUBSTANTIALLY THE SAME SCOPE.

ADJUDICATIONS

IN THE FINAL ANALYSIS, EVEN THE MOST COMPREHENSIVE INVESTIGATION SERVES LITTLE PURPOSE IF THE INFORMATION IT CONTAINS IS NOT PROPERLY EVALUATED AND ADJUDICATED. WE HAVE PLACED CONSIDERABLE EMPHASIS UPON AND ARE CONTINUALLY ASSESSING THE ADJUDICATIVE PROCESS.

THE STANDARD WHICH MUST BE MET FOR CLEARANCE OR ASSIGNMENT TO SENSITIVE DUTIES IS THAT, BASED ON ALL AVAILABLE INFORMATION, THE PERSON'S LOYALTY, RELIABILITY, AND TRUSTWORTHINESS ARE SUCH THAT ENTRUSTING THE PERSON WITH CLASSIFIED INFORMATION OR ASSIGNING THE PERSON TO SENSITIVE DUTIES IS CLEARLY CONSISTENT WITH THE INTERESTS OF NATIONAL SECURITY.

THUS, THE PRINCIPAL OBJECTIVE OF THE DOD PERSONNEL SECURITY ADJUDICATIVE FUNCTION, CONSEQUENTLY, IS TO ASSURE THAT PERSONS SELECTED FOR SENSITIVE POSITIONS MEET THIS STANDARD. THE ADJUDICATION PROCESS INVOLVES ASSESSING THE PROBABLITY OF FUTURE BEHAVIOR WHICH COULD HAVE AN EFFECT ADVERSE TO THE NATIONAL SECURITY. SINCE FEW, IF ANY, SITUATIONS PROVIDE

CONCLUSIVE EVIDENCE OF FUTURE CONDUCT, THE ADJUDICTIVE PROCESS ATTEMPTS TO JUDGE WHETHER THE CIRCUMSTANCES OF A PARTICULAR CASE; TAKING INTO CONSIDERATION PRIOR EXPERIENCE WITH SIMILAR CASES, SUGGESTS SOME PROBABILITY OF BEHAVIOR NOT CONSISTENT WITH THE NATIONAL SECURITY. IT IS CLEARLY A SUBJECTIVE DETERMINATION, CONSIDERING THE PAST BUT NECESSARILY ANTICIPATING THE FUTURE. RARELY IS PROOF OF TRUSTWORTHINESS AND RELIABILITY OR UNTRUSTWORTHINESS AND UNRELIABILITY BEYOND ALL REASONABLE DOUBT.

WHILE EQUITY DEMANDS FAIR AND CONSISTENT ASSESSMENT OF CIRCUMSTANCES FROM ONE SITUATION TO THE NEXT, EACH CASE MUST BE WEIGHED ON ITS OWN MERITS. ALL INFORMATION OF RECORD, BOTH FAVORABLE AND UNFAVORABLE, MUST BE CONSIDERED AND ASSESSED IN TERMS OF ACCURACY, COMPLETENESS, RELEVANCE, SERIOUSNESS, AND OVERALL SIGNIFICANCE. IN ALL ADJUDICATIONS THE PROTECTION OF THE NATIONAL SECURITY IS THE PARAMOUNT DETERMINANT.

OUR BASIC PERSONNEL SECURITY REGULATION (DOD 5200.2-R) DETAILS ADJUDICATIVE GUIDELINES WHICH ARE UNIQUE IN THE FEDERAL GOVERNMENT. THE DOD ADJUDICATIVE GUIDELINES WERE DEVELOPED BY MY FORMER OFFICE IN CONCERT WITH SECURITY POLICY OFFICIALS OF ALL OF THE DOD COMPONENTS. THEY HAVE PROVEN TO BE INVALUABLE TO DOD ADJUDICATORS. INDEED, AFTER THE ISSUANCE OF OUR GUIDELINES, THE DIRECTOR OF CENTRAL INTELLIGENCE DEVELOPED A SIMILIAR APPROACH IN 1980. WE ARE CURRENTLY IN THE PROCESS OF REVIEWING AND COORDINATING UPGRADED GUIDELINES.

DOD COMPONENTS ARE RESPONSIBLE FOR ADJUDICATING PERSONNEL SECURITY INVESTIGATIONS OF THEIR PERSONNEL. SINCE 1976, THE

ARMY AND AIR FORCE HAVE OPERATED CENTRALIZED ADJUDICATIVE ACTIVITIES WHICH ARE CHARGED WITH THE ISSUANCE, DENIAL AND REVOCATION OF SECURITY CLEARANCES. THE NAVY, HOWEVER, CONTINUES ON A DECENTRALIZED BASIS AND HAS, IN EFFECT, SEVERAL THOUSAND CLEARANCE GRANTING AUTHORITIES LOCATED ON SHIPS AND AT BASES AROUND THE WORLD.

REVIEW OF INDUSTRIAL SECURITY PROGRAM

IN LATE 1983, FOLLOWING THE ARREST OF JAMES DURWARD HARPER, JR., FOR ALLEGED ESPIONAGE ACTIVITY, I ESTABLISHED A SPECIAL DOD INDUSTRIAL SECURITY REVIEW COMMITTEE, TO REVIEW THE EFFECTIVENESS AND AMINISTRATION OF THE DEFENSE INDUSTRIAL SECURITY PROGRAM, IN LIGHT OF THE HARPER CASE.

AFTER MONTHS OF INTENSIVE EFFORT, THE INDUSTRIAL SECURITY REVIEW COMMITTEE, OR "HARPER COMMITTEE" AS IT HAS BECOME KNOWN, PRODUCED ITS FINAL REPORT IN NOVEMBER OF THIS PAST YEAR. I HAVE PROVIDED YOUR SUBCOMMITTEE WITH A COPY OF THE REPORT. THEREFORE, I NEED NOT HERE DETAIL ITS FINDINGS AND RECOMMENDATIONS. I SHOULD SAY, HOWEVER, THAT OF THE 25 RECOMMENDATIONS, (A NUMBER OF WHICH RELATED TO PERSONNEL SECURITY), WE AGREE WITH, AND INTEND TO IMPLEMENT, MOST OF THEM. I CAN COMMENT MORE SPECIFICALLY ON THESE ACTIONS IF YOU LIKE, BUT FIRST ALLOW ME TO MENTION GENERAL FEATURES OF THE DEFENSE INDUSTRIAL SECURITY PROGRAM ITSELF. UNDER DOD POLICY, INDUSTRIAL EMPLOYEES MAY BE PLACED IN-PROCESS FOR A PERSONNEL SECURITY CLEARANCE FOLLOWING A DETERMINATION THAT ACCESS TO CLASSIFIED INFORMATION IS NECESSARY IN THE PERFORMANCE OF TASKS OR SERVICES ESSENTIAL

TO THE FULFILLMENT OF A CLASSIFIED CONTRACT OR PROGRAM. THE INITIAL DETERMINATION IS THE RESPONSIBILITY OF INDUSTRY MANAGEMENT. THE POLICY EXPLICITLY REQUIRES THAT INDUSTRY LIMIT THE NUMBER OF PERSONNEL PROCESSED FOR A SECURITY CLEARANCE TO THE MINIMUM NECESSARY TO DISCHARGE CONTRACTURAL OBLIGATIONS.

CONTRACTORS MUST ALSO CERTIFY ON EACH CLEARANCE APPLICATION FORM SUBMITTED TO THE DEPARTMENT THAT THE EMPLOYEE APPLICANT HAS A NEED FOR THE LEVEL OF CLEARANCE REQUESTED, AND THAT PERFORMANCE ON CLASSIFIED CONTRACTS IS REQUIRED.

THE OVERSIGHT RESPONSIBILITY FOR INSURING COMPLIANCE WITH THESE INITIAL CLEARANCE ELIGIBILITY REQUIREMENTS IS SHARED JOINTLY BY INDUSTRY AND DOD. INDUSTRY IS REQUIRED, FOR EXAMPLE, TO APPOINT A SECURITY SUPERVISOR TO MONITOR SECURITY ACTIVITIES ON A CONTINUING BASIS AND TO CONDUCT A FORMAL INTERNAL SELF POLICING AUDIT MIDWAY BETWEEN SCHEDULED DOD SECURITY INSPECTIONS. IN ADDITION, THE DEFENSE INVESTIGATIVE SERVICE, WHICH ADMINISTERS THE INDUSTRIAL SECURITY PROGRAM AND PERFORMS INSPECTIONS OF CONTRACTOR SECURITY OPERATIONS, ALSO OVERSEES CONTRACTOR COMPLIANCE WITH PERSONNEL SECURITY CLEARANCE REQUIREMENTS.

HOWEVER, INDUSTRY SECURITY PERSONNEL AND DIS REPRESENTATIVES REALIZE THE INHERENT DIFFICULTIES ASSOCIATED WITH ASSURING STRICT COMPLIANCE WITH DOD CLEARANCE REQUIREMENTS. THE PRINCIPAL BURDEN TO ENSURE COMPLIANCE RESTS WITH THE DIS INSPECTOR CADRE WHICH CONDUCTS PERIODIC INSPECTIONS OF CLEARED FIRMS BUT HAS A LIMITED CAPACITY TO MONITOR THE VAST NUMBERS

OF CLEARANCE REQUESTS BEING SUBMITTED. AS THE HARPER COMMITTEE NOTED IN ITS REPORT, CONTRACTORS HAVE A POWERFUL INCENTIVE TO INITIATE CLEARANCE ACTION ON AS MANY EMPLOYEES AS POSSIBLE, NOTWITHSTANDING THE REQUIREMENT TO ESTABLISH THE NEED FOR ACCESS BEFORE SUBMITTING A CLEARANCE APPLICATION. UNDER CURRENT PROCUREMENT REGULATIONS, SHORTAGES OF CLEARED PERSONNEL COULD PLACE CONTRACTORS AT A COMPETITIVE DISADVANTAGE RELATIVE TO THE AWARD OF FUTURE CONTRACTS. WE ARE ADDRESSING THIS PROBLEM.

THIS PROBLEM IS NOT RESTRICTED TO THE INDUSTRIAL ARENA. THE NUMBER OF CLEARED DOD CIVILIANS AND MILITARY IS ALSO VERY LARGE, AND WE BELIEVE MANY HAVE NO NEED FOR A CLEARANCE BUT ARE PUT IN FOR ONE OUT OF AN EXCESS OF CAUTION. THIS WAS A MAJOR CONCERN OF THE HARPER COMMITTEE AS IT IS TO US. ACCORDINGLY, WE ARE CONSIDERING, FOR THE FIRST TIME IN THE HISTORY OF THE DOD PROGRAM, PUTTING REQUESTS FOR INITIAL INVESTIGATIONS ON A QUOTA BASIS - WHILE AT THE SAME TIME REDUCING THE NUMBER OF PERSONS WITH SECURITY CLEARANCES TO A LEVEL TEN PERCENT BELOW THE NUMBER REPORTED BY THE COMPONENTS FOR FISCAL 1984. WHILE WE DO NOT WANT TO HAMPER VITAL DEFENSE PROGRAMS, WE BELIEVE THAT SUCH A QUOTA SYSTEM IS THE ONLY EFFECTIVE WAY TO BRING THE BURGEONING VOLUME OF INVESTIGATIONS AND CLEARANCES - ESPECIALLY IN INDUSTRY - UNDER CONTROL.

I NOW WANT TO TURN TO A SIGNIFICANT EFFORT AT THE NATIONAL LEVEL.

REVIEW OF FEDERAL PERSONNEL SECURITY PROGRAM

THE PRESIDENT, IN MARCH 1983 PROMULGATED NATIONAL SECURITY DECISION DIRECTIVE (NSDD) 84 WHICH DIRECTED, AMONG OTHER THINGS, THAT AN INTERDEPARTMENTAL GROUP UNDER THE DEPARTMENT OF JUSTICE (DOJ) UNDERTAKE A "STUDY OF THE FEDERAL PERSONNEL SECURITY PROGRAM AND RECOMMEND APPROPRIATE REVISIONS IN EXISTING EXECUTIVE ORDERS, REGULATIONS, AND GUIDELINES."

THE NSDD-84 STUDY GROUP CHAIRED BY DOJ, AND CONSISTING OF OPM, DOD, FBI, STATE AND TREASURY REPRESENTATIVES, CONDUCTED AN IN-DEPTH REVIEW OF THE MATTER AND ON 1 MAY 1984 FORWARDED RECOMMENDATIONS TO THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS. THESE RECOMMENDATIONS IDENTIFIED AREAS WHICH SHOULD BE ADDRESSED AS FEDERAL POLICY.

WE STRONGLY SUPPORT THIS EFFORT, BELIEVING THAT PERSONNEL SECURITY POLICY SHOULD BE CONSISTENT AMONG EXECUTIVE DEPARTMENTS AND AGENCIES AND OUGHT TO BE GROUNDED IN A COMPREHENSIVE FEDERAL POLICY COVERING CIVILIAN, MILITARY AND CONTRACTOR PROGRAMS.

IT HAS LONG BEEN THE POSITION OF THE DEPARTMENT OF DEFENSE, AND THAT OF SEVERAL OTHER EXECUTIVE BRANCH AGENCIES PLAYING A KEY ROLE IN NATIONAL SECURITY MATTERS, THAT EXECUTIVE ORDER 10450 NO LONGER SERVES ITS INTENDED PURPOSE AND THAT A NEW ORDER SHOULD BE ISSUED. A PRIMARY PURPOSE OF THE NEW ORDER WOULD BE TO DIFFERENTIATE THE PERSONNEL SECURITY PROGRAM FROM THE PERSONNEL SUITABILITY PROGRAM.

ANOTHER PROBLEM HAS ARISEN RECENTLY AS THE RESULTS OF THE MERIT SYSTEMS PROTECTION BOARD, ESTABLISHED TO HEAR CASES

INVOLVING ACTIONS TAKEN AGAINST CIVILIAN EMPLOYEES ON SUITABILITY GROUNDS, INJECTING ITSELF INTO SECURITY CLEARANCE CASES. MS KATHLEEN BUCK, DOD ASSISTANT GENERAL COUNSEL, COVERED THIS MATTER IN DETAIL YESTERDAY--AND I SUPPORT HER POSITION.

PERSONNEL SECURITY RESEARCH

FINALLY, I WANT TO MENTION THAT IN 1983, FOR THE FIRST TIME, WE FUNDED A MODEST APPROACH TO PERSONNEL SECURITY RESEARCH. AT OSD REQUEST, THE NAVAL POSTGRADUTE SCHOOL BEGAN LIMITED RESEARCH INTO SPECIFIC AREAS SUCH AS THE POTENTIAL UTILITY OF PSYCHOLOGICAL ASSESSMENT, EVALUATION OF PERSONNEL INTERVIEW TECHNIQUES, IMPROVEMENT OF THE ADJUDICATIVE PROCESS, AND STEPS TO IMPROVE THE PRODUCTIVITY OF THE BACKGROUND INVESTIGATION. ADDITIONALLY, WE HOPE TO LAUNCH, IN THE NEAR FUTURE, EXPANDED RESEARCH ON THE USE OF THE POLYGRAPH FOR PERSONNEL SECURITY SCREENING.

THESE THEN ARE THE HIGHLIGHTS OF THE DEPARTMENT'S PROGRAM AND OF ONGOING EFFORTS TO IMPROVE IT. THIS SUBCOMMITTEE IS TO BE COMMENDED FOR FOCUSING SOME LONG OVERDUE ATTENTION ON THIS REALLY VITAL BUT OFTEN OVERLOOKED ASPECT OF PROTECTING THE NATION'S SECURITY. I WILL BE PLEASED TO ANSWER ANY FURTHER QUESTIONS THAT YOU MAY HAVE.

AGAIN, LET ME EXPRESS MY APPRECIATION FOR THE OPPORTUNITY TO APPEAR BEFORE YOUR SUBCOMMITTEE.

#1 5/2

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * *

GENERAL RICHARD STILWELL
Deputy Under Secretary of Defense

Accompanied By

BRITT SNIDER
Director
Counterintelligence & Security Policy
Department of Defense

Q. Should there be a single scope of investigation for all levels of clearance if so, what should it be? If not, why?

There should be a single scope of investigation for individuals requiring access to Top Secret and Sensitive Compartmented Information. It seems only reasonable that the nation protect all its most sensitive secrets through a single, rigorous investigative inquiry. This inquiry should include an in-depth interview of the individual covering all aspects of his (or her) history and behavior as it relates to paying bills, using alcoholic beverages or illegal drug substances, and so on. Additionally, we would recommend NACs, checks of state and local police agencies, review of credit information and interviews of professional and personal associates. These checks could then be expanded into other areas as the investigation and history of the subject would dictate.

Q. How do you evaluate the effectiveness of obtaining needed personnel security investigative data from foreign nations? Are there problems? If any, what is being done to resolve these problems?

DOD must rely on the ablity of other U. S. government investigative agencies to gather information in overseas areas where the military departments and the State Department have no investigative authority. It is difficult to evaluate the effectiveness apart from what those agencies tell us and our review of the reports of investigation. We do receive some substantive information which does indicate that some serious attention is being paid to our personnel security requests. Obviously the qulaity of investigative work and availability of investigative information varies from nation to nation. No consolidated evaluation has ever been made as to the quality and availability of investigative information with respect to the individual nations that cooperate in this effort.

There are some problems in terms of timeliness, existence of record information, and priority of the PSI work for another U. S. agency. DIS meets regularly with the parent service in Washington, and occasionally visits some of the units where the backlog is greatest to determine ways to streamline the process, if possible.

Q. NACIs on DOD civilians are conducted by OPM. It is understood that DOD has found it necessary to expand many of these NACIs. Could you comment on this?

It is DOD policy that derogatory information be expanded upon and resolved prior to making a final personnel security determination. Thousands of incomplete NACIs are received from OPM wherein all issues have not been resolved or do not include the subject's version or explanation. DIS is tasked to complete the inquiry. This, of course, adds to an already heavy PSI workload, but resolution of the issues is deemed essential.

Q. It is understood that the DIS backlog and investigative completion times are again rising. Is the solution simply to augment DIS with investigative personnel matching the increased workload?

The DIS pending caseload and the investigative completion times have been rising. There are basically three methods to reduce the pending caseload and improve completion time. First, give DIS more resources to do the additional work. Second, increase productivity of existing resources. Third, reduce the input of new cases. In the FY 86 President's Budget DIS received 177 additional investigative resources for FY 85 and FY 86. Productivity of DIS investigators by FY 86 will have increased more than 4% over FY 84. The input of cases has been partially controlled through a quota system on Periodic Reinvestigations. There is a proposal to extend this quota to initial investigations. We are also conducting a three month test which substitutes a National

Agency Check and credit check for a full field investigation on certain DOD contractor employees who only need a Secret clearance. We feel it is a combination of these three methods, sufficient resources, high productivity and limiting input through quotas that will enable DIS to provide a quality product in a timely manner to all of its requesters.

Q. We note that there is a Naval Personnel Research and Development Center. Is there any similar center in DOD to do personnel security research?

Not at this time. In 1983, I provided $150,000 for an initial effort to develop a personnel security research capability at the Naval Postgraduate School. Since that time some significant strides have been made towards accumulating and integrating security and personnel data cases which have enabled us to conduct a number of very interesting analyses. Much of the work in this area will, of necessity, be accomplished through close coordination with such organizations as the Naval Personnel Research and Development Center.

Q. We understand that OPM has assigned 12 professionals to its personnel investigations staff to do oversight. Your personnel security program is considerably larger than OPM's. How many OSD professionals conduct such oversights?

DOD Directive 5200.2, "DOD Personnel Security Program," charges the Deputy Under Secretary of Defense (Policy) DUSD(P) with the responsibility to "conduct an active oversight program to insure that the DOD Personnel Security Program requirements are complied with."

The Deputy Directorate for Personnel Security (or Personnel and Security Division) -- the principal staff element dedicated to DOD personnel security policy development -- is lodged within the Counterintelligence and Investigative Directorate, ODUSD(P). The deputy directorate is staffed with three professionals and a secretary.

While intermittent oversight visits have been conducted by that staff, the broad workload assigned has prevented conducting oversight of the nature, depth and frequency that is required to ascertain program compliance.

Q. What is DOD reinvestigation policy? What is the reinvestigative scope? Are reinvestigations necessary?

DOD policy is that persons having access to Top Secret, Sensitive Compartmented Information (SCI) and other selected access programs will be periodically reinvestigated. This Periodic Reinvestigation covers a five year period and consists of the following elements:

Review of personnel, security and medical records; personal interview of the subject of the investigation; National Agency Check; law enforcement records; credit check; employment references and appropriate employment records check; developed references, and select scoping as necessary.

Reinvestigations are a necessary part of the investigative process because persons who are cleared may become unsuitable to hold a clearance at a later date. We are continuing to evaluate the productivity and utility of the Periodic Reinvestigation.

Q. How can so may people be cleared? Do they all have need for a clearance? What can be done to reduce these numbers?

DOD policy delegates a fair amount of latitude to components, agencies and organizational commanders in determining the sensitivity of military and civilian positions under their control. While we have no direct evidence that this is being abused, we do suspect that to varying degrees, unnecessary investigations and clearances are being requested by these same authorities. The same situation exists within the industrial security program. Certainly, some of the growth in clearance activity can be accounted for by the more sophisticated and classified pieces of hardware being developed and procured; a good portion of the growth, however, appears unnecessary and avoidable. Short of conducting an in-depth survey of each sensitive position in DOD and industry, we are recommending that Secretary Weinberger impose a 10% cut on clearances and investigations for the 4th QTR FY 85 and all of FY 86 based on FY 84 performance data. This step should help emphasize the fact that clearances and investigations will no longer be freely available to all requesters with no limits.

Q. What ultimately happens as the result of the DOD personnel security investigative process in terms of numbers of denials and revocation of clearances?

> During FY 84, 168,000 Top Secret and 623,000 Secret clearance actions were taken on DOD military, civilian and contractor personnel. Of this total more than 6,000 persons had their clearances denied or revoked. While this works out to less than 1% ratio, another 7,500 personnel did not receive access to classified information due to non-appointment or non-selection to a sensitive position. 102,000 persons were also considered for access to sensitive compartmented information (SCI) with 4,400 being denied such access (4.3%).
>
> There is no national "norm" as to what the percentage of denials/revocations should be for any given personnel security program, however, DOD figures are similar to those found in other federal agencies.

Q. It is understood that DOD enters into agreements to exchange classified information with allied foreign nations. How do you insure that our secrets are passed only to trustworthy personnel under these agreements. In some allied nations, the communist party is a legal politcal party and communist party membership cannot be made the basis of denials of clearance or bar to sensitive positions. How do you insure that members of the communist party are not getting access to U. S. classified information provided under the exchange agreements? Can you explicitly require in such agreements that known members of the communist party shall not be given access to U. S. classified information?

> Nations entering into such agreements provide the United States information on their personel security procedures and permit U. S. representatives to conduct on-the-scene review to insure that their system provides security assurance essentially equivalent to ours. These reviews are reciprocal.
>
> The question of preventing members of the communist party from having access to U. S. classified information in nations where the communist party is a legal party is a sensitive and complicated issue. In this connection, we simply must rely on the security authorities of the nation concerned that U. S. classified information is not compromised.
>
> We cannot explicitly require, under such agreements, that members of the communist party shall not be given access to U. S. clasified information.

Q. What is DOD's position on Basic Installment 311?

Basic Installent 311 is simply the 1984 version of OPM 5-level position sensitivity study effort from which DOD withdrew in 1981.

In March 1982, DOD and other xpected agencies met with Director Devine to discuss the August 1981 "Final Report of the Interagency Study on Implementation of GAO Recommendations concerning the federal pesonnel security investigations program." At that meeting, DOD and the majority of other agencies voiced strong objections to the 5-level approach. At the conslusion of the meeting Director Devine stated that, in light of the objections, OPM was not ready to implement the report, that OPM would distill the major issues, and talk with the agencies again before taking action.

Nevertheless, in Jauary 1984, OPM issued Basic Installment 311 setting forth fundamental revision to Chapters 731 (Personnel Suitability), 732 (Personnel Investigations) and 754 (Suitability Disqualification Actions) of the Federal Personnel Manual without any notice to or coordination with any Federal Agency.

Secretary Weinberger has taken the position that legal and other problems, including excessive costs, identified by our review, necessitate that DOD implementation be held in abeyance until the President has had the opportunity to take action on the recommendations of the NSDD-84 study group which was appointed by him and chaired by the Department of Justice "to study the federal personnel security program and recommend appropriate revisions in existing Executive Orders, regulations, and guidelines."

In the final analysis, we do not support Basic Installment 311. Basic Installment 311 which covers only civilian employees is not the answer to personnel security program upgrading. The NSDD-84 study will assure a deliberate carefully constructed, fully coordinated effort to develop an integrated assessment of all personnel security programs of the Federal government -- civilian, military and contractor employees.

We are confident that, with the full cooperation of all participating agencies, we can recommend to the President, measures that will improve national security.

Q. Is the investigative scope for aliens and immigrant aliens the same as for U. S. citizens?

Immigrant aliens may not be cleared above the Secret level, and the basis for the clearance is a BI. U. S. citizens may be cleared for Secret based upon a National Agency Check (NAC). The scope of the BI for immigrant aliens includes 10 years of traditional leads (e.g., education checks, employment records and interviews, etc.) and an indepth interview of the subject individual, which includes all the elements of the IBI interview as well as specific questions regarding citizenship status and intentions.

Q. How do you ascertain compliance with the DOD program on the part of the DOD components?

DOD Directive 5200.2 provides for conduct of a personnel security program oversight function by ODUSD(P). Unfortunatley, due to TDY funding restrictions, and limited personnel security staff, we are unable to conduct a comprehensive oversight program as we would like. Visits are made when possible to a variety of representative DOD field elements and ongoing contact is effected with security policy personnel in each of the Defense components by means of meetings, correspondence and informal contacts. We do believe there is no adequate substitute, however, for on-the-scene assessment.

Q. How are you controlling investigative requests?

Personnel security investigations are presently controlled insofar as they may only be requested in conjunction with a purpose contained in DOD 5200.2-R, e.g., BI/IBI for a Top Secret clearance, SBI for SCI access, etc. There is presently no cost or quota restriction placed on requesters of PSIs. DIS also screens incoming requests to insure that they conform to policy in DOD 5200.2-R. Those that do not are returned. We currently are staffing a paper that would impose an investigative quota on all components at a level 10% below the number of investiations opened in FY 84.

Q. If a cleared employee of another federal agency transfers to DOD into a position requiring access to classified information, does DOD reinvestigative that employee? If so, at what scope?

If a person transfers into DOD from another federal agency such as DOE, FBI, State or Treasury, their existing personnel security investigation will be honored provided: (1) no break in federal service has occurred greater than 12 months; (2) the level of clearance required is not higher than that previously possessed; and (3) the scope of the previous investigation meets or exceeds DOD requirements. In such instances, we do not feel it is necessary to review the basic investigative file.

The scope of any reinvestigation, if necessary, would depend entirely on the level of clearance required with DOD, e.g., SBI for SCI access, BI/IBI for Top Secret. This arrangement generally works both ways and has proven effective in the past.

Q. The DOD personal history form requires the applicants to list organizational membership including that in the Communist Party. How are your adjudicative personnel able to recognize the significance of such listing with respect to determining the applicant's trustworthiness?

From an investigative standpoint, DIS uses the Encyclopedia of Associations. Volume 1 covers national organizations of the U. S. In addition, inquiries are made to the FBI and other law enforcement agencies concerning organizations. If the organization is known, DIS is provided with its purpose and whether or not its interests are considered to be against the national interest.

When the adjudicator receives the investigation, DIS normally has checked any "unusual sounding" organizations against the Encyclopedia of Associations or runs it through the FBI and expanded as necessary. Since the FBI no longer publishes a list of so-called "subversive" organizations, oftentimes the responsibility falls to the adjudicator's inherent experience, initiative and intelligence. When an adjudicator identifies a "suspect" organization they usually consult with DIS to determine if they or the FBI has any record.

We recognize that our approach to this extremely sensitive matter is not foolproof. We continue to search out ways to insure procedures that are well balanced in terms of individual First Amendment rights and overall national interest.

Q. If all such listings are not forwarded to the FBI, how does the adjudicator determine which ones should be referred to the FBI for guidance?

The profiles currently in use for reviewing the organizational membership are prepared by and obtained from the Justice Department (FBI). As such, only those organizations about which the adjudicator had no knowledge or for which a profile was not available would be referred for additional guidance. Again, there is no standard formula for this as the adjudicator must bring to bear his or her experience and intuition in pinpointing questionable organizations. It also helps if the adjudicator is widely read and the adjudicative organization promotes an in-house training environment to discuss and exchange information in this critical area. When in doubt, the adjudicator can always play it safe and check the organization against the FBI's holdings.

Q. What are you doing about their report?

The Committee's first report included some 39 separate recommendations, 28 of which I have asked to be implemented in whole or in part.

Q. What is the status of the recent General Dynamics security issues?

DIS has been tasked to conduct a total assessment of the security posture of General Dynamics (GD). We have recently completed this task. As a result, it can be said that the overall security posture of General Dynamics, when it is compared to other companies and when the complex nature of the various programs they are involved in is taken into account, is good. That is not to say that individual GD facilities do not have significant problems. For example, at Electric Boat, they have problems in the areas of classification management as well as adverse information. As a result of some current violations we are reviewing involving the Ft. Worth Division, they likewise may have problems in classification management. Furthermore, we have confirmed one case and are currently pursuing our suspicions in a second case involving the "bootlegging" of classified material from government officials to GD marketeers. Finally, we have found indications of excessive clearances at a number of GD facilities. While these problems are serious, and we are handling them appropriately, they are of the type which would not be unique to GD but rather can likewise be found in other large and complex contractor facilities.

Q. Obviously, often certain "minor" scope requirements may or may not be met. Are there any guidelines as to what the cut-off may be before it is determined that clearance may not be issued?

> Investigations are followed through until all required information is collected, or to the point where certain information, which cannot be obtained because of specific circumstances, is determined unnecessary, however, there are no central DOD guidelines on this matter.
>
> In the industrial program, case-by-case judgments are made in these situations, using the DOD Personnel Security Program Regulation and the DISCO Handbook for Adjudication of Industrial Security Clearances for guidance.
>
> In the case of immigrant aliens, where overseas or local information cannot be collected, clearance actions are terminated because of a lack of ability to complete the prescribed investigation.

Q. Are naturalized U. S. citizens cleared under the same investigative scope as native born citizens? If so, does this also apply when the naturalized citizen has lived in the United States only for the minimum period required to obtain citizenship?

> U. S. citizens are subject to the same investigative scope regardless of the basis for that citizenship -- native born or naturalized. The amount of time in the U. S. is not a factor. However, if a person has relatives living behind the Iron Curtain or in an otherwise hostile country, the investigation will be expanded as a hostage case. Additionally, the National Agency Check conducted on people who have lived in foreign countries is more extensive than in the case of a person who has never been abroad.
>
> The question you raise is interesting, however, considering that the scope for an immigrant alien is a 10 year background investigation. On the other hand, a naturalized citizen who has resided in the U. S. five years and one week would be investigated using a 5 year background investigation.

Q. How do you conduct investigations in overseas areas?

The Defense Investigative Service (DIS) tasks overseas Personnel Security Investigations (PSIs) to the U. S. military investigative component (e.g., Naval Investigative Service, Air Force Office of Special Investigations, U. S. Army Intelligence) which is dominant in a particular area abroad. The U. S. Department of State develops personnel security information for us in some areas abroad where there is no military investigative component, relying upon liaison with the host government to obtain the requested information. Results of overseas investigations are incorporated into the appropriate DIS PSI file.

Q. Why did you establish the Harper Committee?

The DOD Industrial Security Review Committee, or Harper Committee as it has become popularly known, was established in the wake of the James Durwood Harper, Jr. espionage case which took place in the Silicon Valley area of California. Originally, the concern was limited to identifying possible policy or procedural shortcomings associated with that specific case. However, shortly thereafter, I decided to expand the Committee's charter to include a review of other espionage cases to assess whether existing policies were sufficient to reasonably thwart or detect such activity. I also directed that the Committee conduct a general analysis of industrial security policies connected with prevention or detection of espionage. I had no preconceived feelings that significant program weaknesses existed, I simply seized the opportunity to avail myself of its member expertise to form a basis for reasonably concluding that they, in fact, did not. A thorough review of that scope of coverage had not been conducted for many years and was, in my view, long overdue.

Q. Is DOD considering expanding personnel security research? What kind of personnel security issues require researching?

> Yes. Since we have been working closely with the Naval Postgraduate School, the Defense Manpower Data Center and the Naval Personnel Resarch and Development Center, we feel it may be appropriate to expand our relationship with the Naval Postgraduate School for future personnel security research efforts. Some of the research areas of interest to us involve:
>
> 1. improving prescreening techniques for high risk jobs;
> 2. developing psychological testing methods to supplement background investigations;
> 3. validation of the most productive elements of the background investigation;
> 4. developing studies on security "failures" in order to assist adjudicators in making better decisions;
> 5. analysis of the strengths and weaknesses of the personnel interview process to develop a strong more effective instrument.
>
> The above are just a sampling of the myriad of possibilities for research in the personnel security area.

Q. What national office or agency has the authority to prescribe what the scope of field investigations -- generically called background investigations -- should be?

What is the authority of the Director of Central Intelligence in this regard?

What is the authority of the Director, Office of Personnel Management, in this regard?

What independent authority does the Secretary of Defense have in this regard?

> There is no national office or agency specifically charged with the authority/responsibility for the overall Federal personnel security program in general, or with prescribing the scope of field investigation in particular.
>
> The Director of Central Intelligence (DCI) is charged by Executive Order 12333 and Section 102 of the National

Security Act of 1947 to ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information and products. In this connection, the DCI has issued Director of Central Intelligence Directive No. 1/14 in coordination with the Intelligence Community, which establishes minimum personnel security standards, procedures and continuing security programs for the protection of Sensitive Compartmented Information.

The Director, Office of Personnel Management, under the provisions of Section 14, E. O. 10450, has been given the authority, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, "to make a continuing study of the manner in which" E. O. 10450 is being implemented.

The Secretary of Defense is designated by Section 133 of the National Security Act of 1947 as the principal assistant to the President in all matters relating to the Department of Defense -- which would include departmental personnel security matters. Moreover, the Secretary is assigned by the Act, subject to the direction of the President, the authority, direction and control over the Department of Defense -- including the separately organized representatives of the Army, Navy and Air Force -- as well as the Defense Components.

Q. What is DOD policy on clearing foreign nationals for access to classified information?

Foreign nationals are not given "clearances" per se. DOD policy requires that every effort shall be made to insure that non-U.S. citizens are not employed in duties requiring access to classified information. When it is determined that such employment in a specific program is necessary in furthering the DOD mission, a "Limited Access Authorization" for classified information may be given under certain conditions:

a. 15 years background investigation must be favorably completed. (If the geographical or political situation prevents sufficiently completed development of investigative information -- access will not be granted.)

b. Top Secret access may be granted only by the personal written authorization of the Secretaries of the Military Departments, heads of DOD Components and certain other limited authorities.

c. Secret and Confidential access may be granted only by certain other designated authorities.

Q. What is DOD policy on clearing immigrant aliens for access to classified information?

Immigrant aliens may not be cleared for Top Secret information. Immigrant aliens, however, may be granted Secret and Confidential clearance based on the favorable completion of a 10 year scope background investigation.

Q. Why must DOD clear immigrant aliens? Why must DOD give foreign nationals even limited access to classified information?

When an individual is admitted to the United States for permanent residence, there is established a presumption that there has been a change of national allegiance from the native country to that of the United States.

Many immigrant aliens bring to the United States certain highly developed skills that serve the national defense effort.

Normally, foreign nationals are given limited access authorization only at the Secret or Confidential level. In the majority of cases, these are persons serving in an administrative or logistical support role in our military installations overseas whose knowledge of the area are exceptionally valuable to mission accomplishment.

Q. What comments do you have on the effectiveness of personnel security background investigations in general?

Personnel security investigations have been effective in screening out the obviously unsuitable from participation in sensitive programs. The introduction of the IBI interview has put clearance applicants on notice regarding the type of behavior that could impact on the clearance decision and is considered an excellent addition to the normal method of conducting background investigations.

Q. What are the major problems in making background investigations more effective?

An increasing reluctance to provide or difficulty in obtaining information necessary for an adjudicator to make an informed decision. This extends beyond getting access to record information -- arrest, juvenile, expunged, child abuse, drug, alcohol -- to individuals providing first-hand information. Those individuals as well as some record custodians expressed fear of lawsuit or other legal action if unfavorable information is provided.

Q. In relative order of priority as to the development of information needed to make personnel security clearance determinations, how would you rank the individual investigative elements?

Today's society is very mobile, more people move, both husbands and wives work and it is difficult to find character references who know the individual being investigated. Because of legislation on Privacy and Freedom of Information, individuals are reluctant to report derogatory information to investigators for fear of reprisal, and employers, schools and other record repositories will release only limited directory type information to investigators. Therefore the personal interview of the subject by a trained investigator is the best source of developed information. National Agency Checks, which include a check of the files of the FBI and other appropriate national agencies, and credit bureau checks are probably the next best sources of developed information. A check of local law enforcement agencies is also productive in developing information but is primarily used to obtain details of an arrest previosuly developed. Other leads are less productive because of the reasons cited above.

Q. Has the Privacy Act of 1974 had any effect on the reporting of adverse information in the industrial sector under the requirements of the Industrial Security Manual?

> We think it has. Although it is difficult to say to what precise degree it has impacted on reports, we have detected a perception on the part of some contractors that they are in some way violating the Privacy Act if they submit reports. DIS has carried out a major education effort to overcome that perception. Attachment shows the growth in the number of 6b(1) reports in recent years.

DISCO - ADVERSE INFORMATION REPORTS

NUMBER RECEIVED

INDUSTRY	622	743	1,257	2,401	1,633	3,266
GOVERNMENT	257	306	375	795	482	964
TOTALS	879	1,049	1,632	3,196	2,115	4,230
	FY 81	FY 82	FY 83	FY 84	1 Oct 84 - 31 Mar 85	Est FY 85

Q. What is the so-called "Company Confidential" clearance? What security checks are required? What is your opinion as to the security effectiveness of Company Confidentials? Should this procedure continue?

> It is a clearance granted by a contractor to U. S. citizen employees who require access to information classified no higher than Confidential. Such a clearance is not valid for access to Restricted Data, COMSEC, Sensitive Compartmented Information, or NATO, except NATO restricted.
>
> The employment records of the employee. Completion of DD Form 48-2, application and Authorization for Access to Confidential Information (Industrial), showing the employee is a U. S. citizen, not a Representative of a Foreign Interest, and no information that reflects suspension, denial or revocation of a clearance.
>
> It is effective as a calculated risk for allowing individuals access to "lower level" information.
>
> Yes. It is a cost effective means of permitting access to "lower level" classified information.

Q. If you do not agree that there should be a single investigative scope, why should there be separate scopes for Senstive Compartmented Information and Top Secret?

Separate scopes for TS and SCI do not make sense. Indeed, our analysis of the IBI versus the SBI currently shows that the IBI is significantly more productive of relevant information.

Q. In your opinion, what is the security assurance difference between the Background Investigation and the Special Background Investigation?

DIS conducted Interview-Oriented Background Investigations (IBI's) and SBI's in 1982 and 1983. The results indicated that the IBI signficiantly out performed the SBI in developing adverse information.

Q. OPM, under its authority derived from E.O. 10450, has delegated to DOD authority to conduct background investigations on DOD civilians. What scope is DOD using for such investigations?

DOD uses the same BI scope that was in existence prior to the implementation of the IBI for DOD civilians. This was done at OPM insistence. For all other BIs, DOD has opted for the IBI which we consider to be a much superior investigation.

Q. Are all requests for personnel security investigations valid requests?

Requests for personnel security investigations are submitted only by authorized requesters defined in DOD 5200.2-R, "DOD Personnel Security Program." These requesters are responsible for making a determination on the validity of requests on persons under their jurisdiction. Under this system, DIS must assume that requests are valid.

During the processing of requests, DIS can, to a limited extent, determine the need for the investigation. Validity of industrial security clearance requests is subject to verification during routine inspection of cleared facilities.

Q. What is DOD policy as to who is authorized to request personnel security investigations? How do you authenticate requesters?

> DOD policy on who is authorized to request personnel security investigations is contained in DOD 5200.2-R "DOD Personnel Security Program," Chapter V. This policy states that requests will be submitted only by those requesters specifically listed in paragraph 5-101 of Chapter V. DIS will only accept requests for investigations from these designated requesters. Other than employing the aforementioned restrictions, DIS has no specific method of authenticating requesters.

Q. How do you insure that persons nominated for clearance truly need access to perform their duties?

> Because of the size and scope of the DOD personnel security program, we must depend to a great extent on the component and agency clearance authorities to faithfully abide by the standards and criteria established in the policy issuances which govern position sensitivity designation and access to classified information. However, because of limited OSD staff resources we are unable to conduct as vigorous an oversight program we would like.
>
> Contractors in the DISP are obligated to organize their work and arrange their facilities so that the least number of employees will request access to classified information. They are also obligated to clear as few employees as possible. Compliance with these requirements is emphasized during DIS inspections of contractor facilities. Included in these inspections is an examination of the contractor's procedures for compliance and a sampling of newly cleared employees to verify that their clearances were requested in connection with an identifiable contractual necessity for access to classified information.

Q. What is the number of personnel holding DOD clearance? At what levels? Civilians? Military? Contractor employee?

A total of 4.3 million civilian, military and contractor employees are cleared at the following levels:

	CIV/MIL	INDUSTRY	RESERVE/ NATIONAL GUARD
TS	454,851	128,405	40,094
S	2,038,984	971,912	345,541
C	13,105	304,904	15,051
	2,506,940	1,405,221	400,686

Q. How many firms have clearances? How do they get them? Do they actually have to have a classified contract with DOD? Can they get a clearance to bid on a contract? What happens if they lose?

As of March 31, 14,145 firms possessed facility security clearances. The clearance process begins when DIS receives a request from a DOD component, from one of the non-DOD user agencies, or from a prime contractor working on a classified program. DIS then must verify that the request is based on an actual procurement which will require the firm to have access to classified information. If the request does not meet this test, DIS will reject it and take no action to clear the firm. The facility clearance must be granted prior to award of a classified contract. In some cases, access to classified information will be necessary in order for a firm to prepare a bid. This is also a legitimate reason to clear a firm. If the firm does not receive the contract, DIS will allow the contractor to retain the clearance temporarily. However, if after six months it is found that the firm has had no use for the clearance, it will be terminated. All of the cleared firms are reviewed for the possibility of termination during the inspection cycle, and unnecessary clearances are weeded out.

Q. Is clearance synonymous with access?

Clearance is not synonymous with access. DOD policy requires that cleared persons be only given access to classified information under strict need-to-know procedures. However, considering the high number of persons cleared by DOD, the potential of inadvertent or unnecessary access is proportionate to the numbers cleared. This is why the department is increasing its efforts to reduce the number of persons cleared.

Q. How often are firms with a clearance inspected by DIS?

As a general rule, the frequency of inspections is based on the level of classified material the facility physically possesses. Firms who possess Top Secret or Secret material are inspected at 6-month intervals. Other facilities are inspected every 9 months. Some service type facilities such as graphic arts firms are inspected every 6 months on the premise that, while classified material is not maintained, it could be in the facility at any given point in time. The Directors of Industrial Security in the Regions may increase the frequency of inspections based on a poor security program. Moreover 12% of the inspections are conducted on an unannounced basis and therefore are ahead of the scheduled interval.

Q. Is centralized adjudication more desirable than decentralized? Where does DOD stand with respect to centralization on Navy adjudication?

Centralized adjudication, in our opinion, is far preferable to the decentralized process for a number of cogent reasons: (1) it provides a single focal point for all inquiries/problems regarding clearances; (2) it affords the agency a rapid means of entering data in the central clearance data base; (3) it eliminates the need to widely disseminate Privacy-sensitive investigation; (4) it provides an economy of scale by locating all adjudicators at one spot; (5) it promotes the professionalism of adjudicators through improved training and cross-fertilization of ideas; (6) it enhances the accuracy and soundness of clearance decisions by concentrating the function in the hands of a trained professional body rather than an additional duty; (7) it insures that correct application of an individual's due process rights.

DOD continues to strive to persuade Navy of the benefits of central adjudication, as practiced by the Army and Air Force. While the Navy has centralized adjudication for SCI and most of their civilian they continue to oppose its further expansion.

Q. If there is a significant question about a person's trustworthiness after obtaining access, does the person continue to have access until a final adjudicative determination is made? Is there a provision for suspension of access in the interim?

Whenever a serious question arises about the trustworthiness of a person subsequent to the issuance of a security clearance, action is normally taken to suspend access pending a final adjudicative determination. Usually the employing activity initiates the appropriate inquiry to gather all relevant factors relating to the subject's problem or behavior, to include an interview of the subject and then submits the material for adjudication. The security clearance may then be revoked or, in some circumstances, reinstated depending on the nature and seriousness of the behavior. In the vast majority of cases, the person's access continues until the case is finally adjudicated.

In the contractor field, whenever continued access by a cleared individual poses a threat to the national security, that individual's clearance may be suspended on an interim basis. The Industrial Security Regulation authorizes the Director, DIS, to take this action, when appropriate. This action is, of course, not taken capriciously. In FY 84, with the concurrence of DUSD(P) and OGC, 29 actions were taken by the Director, DIS.

Q. What do DOD personnel security investigations cost? How does this compare to other federal agencies?

In FY 84 the average Special Background Investigation (SBI) is estimated to have cost about $600 while the average Interview-Oriented Background Investigation (BI) is estimated to have cost about $400. These estimates are based on the Defense Investigative Service's FY 84 obligations and estimates of non-reimbursed costs. These cost estimates do not include adjudication costs or estimates of lost productivity for the individual being cleared. Office of Personnel Management (OPM), effective February 1984, was charging between $1,675 and $2,125, for the equivalent of an SBI depending on the time period in which the investigation was to be completed. OPM does not conduct IBI type investigations.

Q. Similarly, for intra-DOD reassignment of cleared personnel is reinvestigation required by DOD policy?

Since personnel security investigations within DOD are conducted by DIS at a standard scope and all DOD components employ uniform DOD adjudicative guidelines, a great deal of time, effort and cost is saved through a policy of mutual and reciprocal acceptance of clearances. This policy does not apply to special access programs or when there is an indication that the person needs access to more sensitive information than that for which the clearance was initially issued. Also if a person's previous investigation at the time of transfer is more than 5 years old, a periodic reinvestigation may be conducted.

Q. Is the DOD personnel security program sufficiently funded?

With respect to the investigative effort, with the additional resources in the 1985 President's Budget, a quota system to control the input of initial and periodic reinvestigations and elimination of full field investigations for certain Secret security clearances, DIS is sufficiently funded to accomplish their portion of the DOD personnel security program.

However, at present, DOD does not separately budget for the remainder of the personnel security program such as the adjudicative process and the administrative support to processing clearance requests and maintaining continuing security evaluation.

Q. How does DOD view special access programs? As good or bad? How do you control them? Are we sure they are getting the best security?

The Department's position, based upon our best intelligence, is that special access controls are effective and necessary in safeguarding from the Soviets our intelligence sources and methods, our special operations, and our particularly sensitive research and development. Special access controls are designed to limit the number of persons with access to the minimum essential to achieve the objectives of the program. Need-to-know, in most cases, is determined by a single authority -- usually, the Program manager. Enhanced physical and technical security requirements may be applied. Carve-out contracting techniques may be used to protect the existence of a program. These more stringent safeguards appear to be more effective than normal safeguards. In short, they appear to be achieving their purpose.

Q. Have you considered contracting out personnel security investigations as a means of relieving DIS wheh workload exceeds DIS investigative resources?

We are continuing to study this possibility.

Q. Some years ago, a "Blue Ribbon Panel" made certain recomendations concerning personnel security in DOD. Are they being implemented?

Action has been taken with respect to many of the recommendations made by the Blue Ribbon Panel. For example, the Interview-Oriented Background Investigation (IBI) has been expanded, the moratorium on Periodic Reinvestigations has been lifted and the scope of PRs expanded, and, research has been initiated into the potential value of psychological assessment as part of the personnel security investigative/evaluative process. Additionally, with respect to the use of the polygraph, the Panel recommended uniform use of the polygraph for both civilian and military personnel at NSA, institution of a screening polygraph for personnel assigned to critical intelligence positions with DIA, and use of a counterintelligence-scope polygrpah examination as part of the reinvestigation process for a limited number of persons who hold extra-sensitive assignments.

As a result of several hearings before a number of committees and subcommittees of both the House and Senate as well as extensive discussions with members and staffs of various Congressional committees and subcommittees, the Congress of the United States has, in enacting the FY 85 Defense Authorization Act authorized the Department to conduct a one year test, limited to 3,500 persons, of a revision of DOD polygraph policy that would accommodate the use of the polygraph recommended by the Panel.

Q. Similarly, a House Appropriations Committe report of 1975 made comments concerning desirable actions by the DOD. What is the status of these directed actions?

In 1975, the House Appropriations Committee, in connection with its consideration of appropriations requested for DIS in FY 86, directed that its Surveys and Investigations staff conduct a review of DIS. As a result of this review, the Appropriations Committee reduced the funds to DIS by $6,440,000, reduced travel funds by approximately $145,000, reduced DIS authorized manpower by 765 spaces and recommended that OSD initiate a review of DIS with the objective of improving management and operations and, recomended that all military positions be civilianized.

An in-depth management survey of DIS was conducted by the Defense Audit Service at the requst of the DUSD(P). The DAS interim report of this review, No. 82-034 and final report, No. 82-084, found that significant improvements had been made in basic management policies and practices.

With respect to civilianizing miltiary positions, in 1975 DIS had approximately 1,000 military personnel. At present there are 11 military personnel in DIS field elements and 2 at the Headquarters. These remaining military personnel will be phased out by the end of this Fiscal Year.

Q. Last year, Congress authorized a polygraph "test program" for DOD in personnel security screening. Comments? Status? Prospects for use of polygraph?

In enacting the FY 85 Defense Authorization Act, Congress authorized the Department of Defense to conduct a one year test, limited to 3,500 persons, of its proposal for use of a counterintelligence-scope polygraph examination to assist in determining the eligibility of DOD civilian, military and contractor personnel for access to specifically designated classified information protected within special access programs; employment, assignment, or detail to critical intelligence positions within DIA; and interim access to Sensitive Compartmented Information. The Department has promulgated the guidance necessary to administer the test program, nominations for participation are being received from the DOD components, and arrangements are proceeding for the actual conduct of the examinations. It is believed that the test program will reflect that value of the polygraph as a supplement to the personnel security investigation and a deterrent to those who might otherwise consider involvement in espionage directed against our most sensitive classified programs and activities.

Q. Industry complains of long delays in putting employees to work in classified projects because of failure to receive clearances within a reasonable time. Is anything being done to improve this situation?

The problem essentially has been due to (1) heavy workload and (2) inadequate resources at the adjudicative level handling serious derogatory cases. We have been able to improve this situation by assigning additional personnel to adjudicate these cases and through making significant improvements in procedures. Most recently, however, we have centralized all adjudication under a single manager in order to increase efficiency and effectiveness throughout the process.

Q. It is regularly alleged that a problem underlying delayed investigations is that to many employees need clearances because there is too much classified information. Is there anything being done about this problem?

With OSD coordination, the Defense Investigative Service, on 15 March 1985, issued an Industrial Security Bulletin (ISB 85B-1) that addresses one aspect of this question. Almost exclusively, this Bulletin is devoted to the need to reduce the number of personnel security investigations and resulting security clearances. The Bulletin details some actions taken that have in fact avoided the initiation of needless investigations and subsequent issuance of security clearances. Also mentioned in this Bulletin, which has wide dissemination, is the need to provide more precise security classification guidance which will tend to reduce the amount of information being classified. On a separate front, the Deputy Under Secretary of Defense (Policy) has issued a revised Chapter XII, DOD 5200.1-R, "Information Security Program Regulation" that specifies more rigid control on the creation of Special Access Programs and approval of "carve-out" contracts. It is anticipated that this action too will tend to reduce the amount of highly classified information that is being created. Further, Directorate of Security Plans and Programs staff conducts Information Security Program reviews at DOD activities and DOD contractor facilities. A primary focus of these reivews is on security classification guidance.

Q. Have carve-out contracts contributed to the increased workload for DIS and, if so, to what extent?

I believe that so-called carve-out contracts have had an impact but I do not believe that they have had a signficiant impact. Although carve-out contracts have grown in number over the past ten years, they still comprise less than 5% of all classified defense contracts. (More than 67,000 classified contracts were made last year.)

Moreover, even if these contracts were not "carved-out," they would still be classified and thus would still require a favorable adjudication of background investigations and national agency checks as a prerequisite for access.

Under Defense regulations, DUSD(P) has authority to approve enhanced personnel security requirements for particularly sensitive (or special access) programs. But I have seldom exercised this authority. Where enhanced personnel security has been approved, the additional safeguards were justified by the sensitivity of the program.

Q. What are carve-out contracts?

Carve-out contracts, sometimes called "black" contracts, are contracts that support particularly sensitive programs approved individually by the Secretary of a Military Department, the Director, NSA, or the DUSD(P), as appropriate. Under new DOD policy contained in Chapter XII to the Information Security Program, 5200.1-R, carve-out contracting techniques should not be approved unless mere knowledge of the existence of a contract poses an unacceptable risk of compromise to a special access program.

Q. What has DOD's experience been with the quality and timeliness of OPM investigations?

OPM conducts primarily National Agency Checks with Inquiries (NACI) for DOD civilians entering non-sensitive or non-critical sensitive positions. It has been our experience that NACI's are now taking up to 6 months to complete (vs 45 days for DIS NAC and 91 days for BIs/SBIs) and thousands are often returned without appropriate expansion of adverse information. Moreover, NACIs are closed out by OPM as "adverse" when they contain only very minor adverse information, such as failing a course in college, or when a written inquiry is returned as undeliverable. Others with significant adverse information, such as arrests or drug use, are returned by OPM to the requester without expansion and subsequently sent to DIS for expansion. In cases such as these it could take several months for a final adjudicative determination to be reached.

Q. Should Executive Order 10450 be continued in place, revised or superseded?

We have long felt that E.O. 10450 no longer serves its intended purpose and that a new order should be issued. This is one of the primary options under study by the interdepartmental working group established under NSDD-84. The working group also has under consideration recommending a new Executive Order, separate from E.O. 10450, which would establish uniform personnel security standards and criteria for all persons (civilian, military and contractors) requiring access to classified information or assignment to sensitive national security positions.

Q. When it is considered to serve the national interest to clear persons outside the federal government (excluding national security contractors) what investigative requirements apply to such persons?

Executive Order 12356 provides that a person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes. DOD Regulation 5200.1-R, Information Security Program Regulation, provides that a person may be given access only if there is a demonstrated need for access and a determination has been made of that person's trustworthiness. This determination shall be based on an investigation in accordance with the standards and criteria of DOD Regulation 5200.2-R. The investigative requirements shall parallel the various levels of security clearance.

Q. What effect has the Family Education and Privacy Act of 1974 had upon DOD obtaining information relevant to personnel security determinations?

The Family Education and Privacy Act of 1974 has restricted the release of information to only "directory" type information (dates of attendance, major field of study, and confirmation of graduation) without a release authorization. This has made substantive information more difficult, but not impossible, to obtain. There has been a reluctance on the part of school administrators, however, to provide disciplinary or other types of files which contain information which may be potentially disqualifying.

Q. What is DOD policy with respect to continuing evaluation of a person's trustworthiness after being cleared? How effective is your continuing evaluation system? Is the system uniform with respect to DOD civilians, members of the armed forces and cleared contractor employees?

DOD policy is that the issuance of a personnel security clearance or the determiantion that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, a cleared person's trustworthiness is a matter of continuing assessment. DOD places responsibility on commanders/organization managers and supervisors to evaluate on a continuning basis the status of personnel under their jurisdiction with respect to security eligibility. Programs have been set up to insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within an organization is considered in the personnel security review process.

This system covering DOD civilian and military members has been highly effective. In fact, the great majority of clearance revocations and access withdrawals is based on information developed through this kind of continuing evaluation.

While the approach is not identical to industry, there is a requirement for cleared facilities to report to DOD information that raises question as to the continuance of a contractor employee's clearance. This constitutes an important feature of the industrial program. In all frankness, however, the reporting from contractors has not reached the volume or level of candor found in the DOD civilian/military continuing evaluation system.

Q. Deputy Secretary Carlucci in a policy memorandum dated August 6, 1982 required that, as part of the periodic reinvestigation, supervisors would review an updated personal history statement and certify whether or not he/she was aware of relevant derogatory information not reported by the person to whom the personal history statement applies. Was this implemented? If not, please explain.

Implementation of the August 6, 1982 Carlucci memorandum involved use of the a periodic, random counterintelligence-type polygraph for access to Sensitive Compartmented Information. When the Congressional moratorium on expanded DOD use of the polygraph was incorporated in the FY 84 Defense Authorization Act, for all practical purposes, the Carlucci memorandum became non-operative.

We still have under consideration procedures that will involve supervisors even more in the continuing security observation process than at present.

Q. If you do not recommend a single scope investigation, what should the scope for Secret be?

We recommend a single scope -- consisting of an IBI -- for Top Secret and Sensitive Compartmented Information. We defer to the forthcoming determinations of the NSDD-84 study group as to what should be done for Secret.

Q. What is the level and frequency of oversight performed by your office over the DOD personnel security program? How effective is it?

DOD Regulation 5200.2-R charges us with oversight of this program. However, due to limited personnel resources and travel funds, we are unable to conduct oversight visits to the field as frequently as we believe necessary. For example, the first oversight visit to DOD facilities in Europe will begin later this month. No visits have been made to DOD units in the Pacific in recent memory. Most personnel security oversight visits are conducted in the United States, with the majority concentrated at available locations in the Washington area. Visits to Defense Investigative Service (DIS) Headquarters and field locations are conducted occasionally to evaluate their progress and productivity. Regular contact is maintained in the Washington area with component security policy personnel responsible for implementing DOD security policy.

Q. Does DOD designate various levels of position sensitivity?

All civilian employees with a DOD security clearance, depending on level of clearance, are considered to be in either a critical-sensitive or non-critical sensitive position. Military and contractor personnel possessing a security clearance are, by definition, considered to occupy sensitive positions although they are not formally designated as such like civilians.

Q. Do you require the DOD components to account for and report the number of clearances they issue? Do they account for and report the number of personnel with continuing access?

Each year all DOD components must report to OSD the number and type of clearances issued the previous year, the number of adverse actions taken as well as a breakout, by level of currently cleared personnel. No report is made of those persons actually receiving access to classified information.

Q. Adjudication is a key element of the personnel security clearance process. How does DOD insure quality adjudicators?

DOD adjudicators, for the most part, are selected from the ranks of the security community with expereince in personnel security investigations, counterintelligence and criminal justice. Ideally, candidates for such positions should possess qualities of maturity, intelligence, experience and common sense to succceed in the adjudicative field. There are few quality training courses around to serve the needs of new adjudicators.

We do not subscribe to the OPM course in that OPM, over the years, has placed stress upon suitability criteria. Moreover, OPM stresses "nexus" with respect to the suitability standards whether employment of the individual "promotes the efficiency of the service."

Through the centralized adjudication concept in DOD adjudicators receive close supervision from more experienced personnel and can be more easily cross trained in the various facets of this important discipline.

Q. What training do DOD adjudicators undergo?

While there are, at present, no formal DOD training courses for new adjudicators, most have had some previous experience in security related disciplines. Senior adjudicators with the Army and Air Force central facilities conduct in-house training supplemented by attendance at a one-week course conducted by the DCI Security Committee. With the exception of the Naval Civilian Personnel Command, Naval Security Group and Naval Intelligence command, Navy adjudications are conducted at several thousand locations by persons who often have little or no security adjudicative background.

Q. Are there DOD adjudicative training standards?

Not at present. One of our long range goals is to develop an improved capability to select, train and evaluate DOD adjudicators. The Air Force is working with a behavioral scientist in this area right now and we hope to begin planning a recurring DOD adjudication course to serve the needs of the DOD adjudicative community in the near future.

Q. Should there be a central federal personnel security adjudication training facility?

We endorse such a concept for adjudication of personnel security as against suitability cases. DOD sponsored a DOD Adjudicator's Conference a few years ago and we have plans for sponsoring others in the future.

Q. What is DOD policy vis-a-vis due process procedures for personnel security adverse determinations?

Basic policy is set forth in DOD Regulation 5200.2-R, DOD Personnel Security Program. Essentially, no adverse personnel security action may be taken unless the person concerned has been given:

a. A written statement of the reasons why the adverse action is being taken;

b. An opportunity to reply in writing;

c. A written response stating the final reasons upon which the action is based (if the action taken is still adverse); and

d. An opportunity to appeal to a higher authority.

These procedures apply to DOD civilian and military members.

Due process procedures for contractor employees are essentially the same, except that as provided for in DOD Directive 5220.6, Industrial Personnel Security Clearance Program, the applicant is additionally offered, (1) an opportunity to appear personally before the head of the department or his designee and (2) an opportunity to cross-examine persons either orally or through written interrogatories who provided information adverse to the applicant.

Q. The due process procedures for DOD civilians and military set forth in DOD Regulation 5200.2-R appear to be more streamline than those afforded contractor employees under DOD Directive 5220.6. Can you explain why they are different?

The due process procedures employed in the Defense Industrial Security Programs were developed as the consequence of the 1959 Supreme Court Decision in Green v. McElroy. Miltiary/Civilian due process procedures reflect minimal process required by the Supreme Court in other decisions.

Q. If an investigation is opened on a cleared member of the armed services, or DOD employee, based on derogatory information bringing into question the subject's trustworthiness, is the subject's immediate supervisor notified so that steps may be taken to monitor the person or prevent compromise?

Inasmuch as the majority of issue type investigations opened by DIS on cleared employees are initiated by the employing organization, it is likely that appropriate notifications and precautions have been taken locally. Depending on the seriousness of the allegations, the employee may have his security clearance suspended pending the outcome of the investigation. Such a decision usually involves the supervisory chain of command. If access is not suspended, it is the responsibility of the local security manager, in concert with the supervisor, to take appropriate measures to insure that the integrity of the classified material is maintained.

Q. Are all elements of the DOD personnel security program, including investigations, adjudication, processing of clearance requests, issuance of clearances, etc., identified and incorporated into the DOD budget process?

Personnel security investigations and industrial security clearance processing, including adjudication, are covered in the Defense Investigative Service budget. Other elements of the program are not identifiable presently in the DOD budget process.

Q. It is understood that since 1982, DIS has been conducting GAO's background investigations. Can you comment on the reason GAO wants DIS to do its investigations instead of OPM?

Investigations conducted by OPM for GAO did not resolve derogatory or adverse information. Information developed during the course of an OPM investigation was left to the GAO to resolve. OPM did not provide Subjects an opportunity to refute or explain any adverse information because they did not conduct a Subject Interview (SI).

DIS is also much less expensive and more timely. A DIS BI costs $500; an SBI costs $800; and we average between 60-75 days completion time. OPM bills at the rate of $1,825 to complete a BI in 35 days; $1,525 to complete a BI in 75 days; and $1,375 to complete a BI in 120 days. For SBIs, its costs $2,125 for 35 day service; $1,825 for 75 day service; and $1,675 for 120 day service.

Q. Giving that a major period of the required investigative scope covers a locale where investigative record checks are not available, would DOD still issue clearance?

> While this is not a common occurrence in the United States, it does occur with some frequency with respect to local agency checks, as well as in overseas locations. If a significant portion of a person's life is not covered by the investigative scope and cannot be verified by other means (e.g., polygraph), then a security clearance should not be issued. If the scope has been substantially met with only minor omissions, and the results are favorable, a security clearance may be issued if the adjudicators determine that no threat is presented to the national security. However, DOD investigators are finding that usually reliable sources of information are becoming increasingly unproductive as a result of Privacy considerations, a fact which will make it more difficult in the future to render sound clearance determinations.

ADDITIONAL QUESTIONS AND RESPONSES FROM GENERAL STILWELL

QUESTION: Your statement mentions that DoD is considering using a quota system on clearance requests. Could you explain how that will work and when it will be implemented.

ANSWER: DoD is considering using a quota system to bring clearance requests under control, but such a system has not yet been approved by the Secretary. If such a plan were approved, it might be implemented along the following lines.

In the industrial area, new contractors cleared for participation in the Defense Industrial Security Program (DISP) would be required to negotiate their anticipated personnel security clearance requirements with their respective Defense Industrial Security Cognizant Security Office (CSO). For contractors already in the DISP, new clearance requests would not be accepted until such time as existing personnel security clearances had been reduced by 10% of a benchmark figure of existing clearances at a specific point in time. Any exception to this policy would initially require the submission of a justification statement, with final approval authority resting with the CSO. This quota system would be implemented in two stages. Quotas would initially be established for TOP SECRET clearances and later applied to SECRET clearances. Dates of implementation are currently projected for October 1, 1985, and April 1, 1986, respectively.

For military and civilian personnel, each DoD Component would be required to curtail the number of investigative requests by a set percentage of their 1984 volume. The Component would have to allocate for FY 86 the requests to its various elements based on known requirements and program priorities. At present the percentage is planned to be 10% of 1984 actual requests.

QUESTION: Should contractors be required to recertify the need for an employee's clearance every five years?

ANSWER: Yes. Experience has proven that after initial certification as to the necessity for an employee's clearance, there is then a breakdown in the contractor's system of review of the necessity for continued access. Consideration is being given to establishing a requirement for the contractor to maintain a "justification record" at the facility for review by DIS which would contribute to enforcement of the requirement to administratively terminate unnecessary personnel security clearances.

QUESTION: According to the Harper report, it would take DIS a decade just to perform the update investigations required as of the end of 1984. In light of those manpower restraints, should contractors require their personnel to complete an updated personnel security questionnaire every year?

ANSWER: No. We do not feel such a practice would serve a useful purpose. The passage from the Harper Report about which you refer concerned only employees cleared Top Secret and those authorized access to Sensitive Compartmented Information (SCI). The decade projection was based on a calculation keyed to existing investigative resources and PR workload. As mentioned in response to the preceding question, we intend to significantly reduce the PR workload by altering the present system to place focus on those having actual access rather than the existence of a particular level of clearance or authorization for access (SCI access list). Accordingly, if the Harper Committee estimates concerning Top Secret (TS) cleared contractor personnel who have never had TS access or only infrequent access are resonably accurate, and we believe they are, the related PR workload could be reduced substantially. Therefore, the current PR backlog could be accomplished in considerably less time.

QUESTION: Why does DoD require contractors to hire employees before they are cleared? Doesn't this present productivity and personnel problems for the contractors who then must await a clearance decision before utilizing the employee fully?

ANSWER: Two reasons. Namely to protect against unwarranted invasions of privacy and to safeguard against an even greater clearance proliferation problem than we now face. The DoD is proscribed from conducting such investigations and the collecting or storing of information on persons with no affiliation or connection of any kind with the Department of Defense. To initiate investigative action on prospective employees who might reasonably never become employed by a contractor would be ill-advised and exceedingly costly. In response to the second part of this question, the answer is yes. The solution, however, is not to process prospective employees for a personnel security clearance, but rather to bring inordinately long and unacceptable processing times into line. The Harper Committee recommendations regarding the expanded use of interim processing procedures and adoption of "one-time" access authority may very well prove to be the answer. We intend to try both approaches.

QUESTION: In both the Harper and the Boyce cases, substantial number of documents were removed and copied after-hours. Does DoD plan to implement the Harper report's recommendation that contractors be required to monitor after-hours access? If so, how?

ANSWER: We intend to implement the Harper Committee recommendation to tighten after-hour controls precisely as suggested. But while the after-hour problem may be more acute, physical security enhancements must also be placed into effect during normal working hours as well. While we have tasked ourselves to develop the general policy, the specific control measures to be required must necessarily be worked out on a case-by-case basis between individual companies and the Defense Investigative Service (DIS). As you know, the DIS has been delegated responsibility to administer the Defense Industrial Security Program, and that agency's inspector cadre would assess conditions and needs, preparatory to jointly arriving at the precise requirements needed to satisfy the general policy.

QUESTION: I believe you were present for the testimony of Christopher Boyce last Thursday. Mr. Boyce, who was convicted for successfully removing highly classified documents from TRW, offered eight recommendations to improve personnel security. I'd like to briefly paraphrase those and ask you to comment.

-- Closer supervision over compartmentalized special access projects.

ANSWER: The Department of Defense has a Special Access Programs Working Group. One objective of that Working Group is to develop policies and procedures that will provide the best possible security for particularly sensitive programs. Special access programs often impose a "Two-person Rule" requiring the presence of two individuals anytime particularly sensitive information is being handled. We need to strengthen the security inspections for these programs to ensure that such requirements are faithfully implemented. I am advised that the Working Group has been provided a copy of Mr. Boyce's statement made before the Subcommittee and that it will be circulated to DoD Special Access Program managers and others responsible for security of these programs. I anticipate that it will become a part of the continuing security education program.

-- Required inspection of every package, brief-case, etc.

ANSWER: We do not support inspection of every package, brief-case or parcel carried from a particular building or cleared facility. Such a practice, if placed into effect, would be highly disruptive and counterproductive in many ways. We do, on the other hand, support and intend to implement the related

Harper Committee recommendation on the subject. As you know, the Committee supported random or spot checks of briefcases and the like. The key is to instill an enhanced sense or awareness of security in the workforce and to subject every item carried from a building or plant to possible search. The random or selected (profile or for cause) approach is preferred over the total audit concept championed by Mr. Boyce.

-- Metal detectors.

ANSWER: The use of metal detectors was recommended by the Harper Committee as one possibility to tighten perimeter security at cleared contractor facilities. However, as that Committee thoughtfully pointed out, the solution is not to impose a single control measure across-the-board. The needs and vulnerabilities of the 14,000 plus cleared facilities differ and requiring the use of metal detectors would be ridiculous if imposed on all. For example, a firm that elects to impose mandatory searches of all parcels would not look kindly on purchasing metal detectors, a less effective security measure. We support the Harper approach, i.e., review each firm's existing security measures and supplement as unnecessary, by continuous or intermittent means, to create a condition "capable of preventing or detecting physical presence, unauthorized access, and removal of classified material from the premises."

-- Use of encoding devices on classified elements.

ANSWER: The use of encoding devices on classified documents would be available as an option using the above approach.

-- Polygraph examinations upon an employee's termination as well as at the time of an update investigation.

ANSWER: The Department supports the concept that the polygraph can, when properly controlled and administered by well-trained, competent examiners, be an effective tool in deterring and detecting espionage. In this regard, it is noted that the FY 85 Defense Authorization Act authorized the Department to conduct a one-year test, limited to 3,500 persons, of its proposal for use of a counterintelligence-scope polygraph examination to assist in determining the initial and continued eligibility of DoD civilian, military, and contractor personnel for access to specifically designated classified information protected within special access programs; employment, assignment or detail to critical intelligence positions within the Defense Intelligence Agency; and, interim access to Sensitive Compartmented Information.

However, polygraph examinations in the magnitude and scope implied by your question would never receive the approval of the Congress and, moreover, would far exceed DoD resources.

-- Increased and expanded on site inspection by the government.

ANSWER: We agree in principle only. The DIS has, over the past couple of years, been heavily involved with a formal program of enhancing the scope and quality of its inspection effort. Other similar initiatives have occurred over the years, all designed to assure, to the extent possible, that only quality, in depth inspections are conducted. Although quality has always been stressed, the question of frequency has not been much of an issue. Moreover, the frequency of inspections is clearly secondary to quality considerations. As a matter of fact, the Harper Committee reasoned, quite soundly, that many contractors are being inspected too frequently. We agreed and are now revising the basic schedule along the lines recommended. It may be that the truly sensitive facilities will be subject to increased inspection efforts under the new schedule. We might add that the government inspections referred to by Mr. Boyce at building M4 were not based on the inspection schedule reviewed by the Harper Committee, nor were they conducted by DIS representatives.

-- A system of anonymous complaints on security breaches directed to the government and not the company.

ANSWER: We have reached tentative agreement with the Inspector General, DoD, to expand formally the present DoD Fraud, Waste, and Abuse Hotline to include reports of security violations. The details of staffing and implementing the expanded systems are currently being worked out. We did not agree with the Harper committee recommendation that a separate Hotline, be established within the Defense Investigative Service, a much costlier proposition. The expanded IG Hotline would facilitate, and in fact encourage, the direct receipt by the government of complaints on security breaches rather than staffing them up through industry channels as is now the case.

QUESTION: Mr. Boyce also testified that current security briefings do not sufficiently convey how espionage, in his words, "wounds a man." Instead, he believes briefings incorrectly stress the supposed excitement and intrigue of espionage. Would you comment?

ANSWER: Mr. Boyce incorrectly characterizes our security briefings as glamorizing the act of espionage. If he felt excitement and intrigue during his ill-fated association with Soviet intelligence operatives, this feeling was not derived from any intelligence or security briefing administered by the Department of Defense. Rather his viewpoint can be more genuinely attributed to fictional and distorted motion picture and television accounts of such abhorrent activity. Nonetheless, we do not doubt his sincerity in making such a statement. More importantly, however, is that others may share Mr. Boyce's misconception on the subject. It may be that more should be done to stress the less desirable aspects of the business and the personal harm and anguish that often results.

Nevertheless, we intend to obtain a copy of the audio-visual tape of Mr. Boyce's testimony for use in the DoD security clearance program.

QUESTION: Should contractors be allowed access to the privacy portion of clearance applications as part of a "prescreening" process?

ANSWER: Definitely not. Prior to 1966 contractors reviewed the entire application for clearance (PSQ), including the information now described under the privacy portion of the PSQ. During this period employees were reluctant to reveal adverse information in their background since they realized it would become known to the contractor who could take precipitous action adverse to the employee.

It is DoD experience that the most reliable source of adverse information, is the person who is being processed for the security clearance. Since the adoption of the privacy portion to the PSQ in 1966, individuals freely reveal adverse information in their background, fully convinced that it is information going directly to the Government to be used exclusively in determining eligibility for a security clearance. As a result of the privacy portion and the privilege provided, adverse information is made available to the Government which in all probability would not have become known through typical investigative efforts. In any event, if the prohibition against contractor review was removed, it could be reasonably concluded that employee applicants would be more inclined to withhold pertinent information out of fear of employer reprisal than because of dishonesty or intent to deceive the Government.

QUESTION: The Harper report notes that from 90,000 to 95,000 of contractor personnel cleared for Top Secret information did not have frequent access to top secret information and that 35,000 to 40,000 never had access to such information. What can be done to reduce the number of clearances to only those that are truly necessary?

ANSWER: Two things: Namely enhanced initial industry and government screening procedures and greater after clearance oversight to assess continuing need. The Harper Committee recommendations regarding use of the Clearance Justification Data Sheet and automatic downgrade or termination action may be effective in that respect and both are under favorable consideration. Implementation, however, depends on adoption of other proposals now being considered. One difficulty to overcome is that a personnel security clearance, and the higher the better, is perceived by many as a valuable employment and promotion asset. Industry can be expected to oppose any measure aimed at closer government scrutiny in this regard. It is vital that we involve top management in any new procedure and that such individuals lend their active support to any related initiative. In this regard, action has been initiated to amend procedures to require executive management officials to become personally and directly involved in reviewing requests for Top Secret clearances being submitted to the Government.

QUESTION: We heard testimony that cost competitive contracts provided contractors with a "disincentive" for strong security measures by including security costs in computing the bid. Do you agree and if so, what can be done to correct this?

ANSWER: There is undoubtedly some truth to this allegation. The ISM is usually more than adequate in conveying effective security measures to industry. If more extensive measures are needed, such as specialized areas or devices, separate funding may be provided. Should a contractor determine that additional security measures are essential, this fact and the supporting rationale should be made known to the contracting activity. The bid response need not include these additional costs however. The larger problem, especially as concerns classified programs outside the inspection auspices of the DIS, may be the imposition and funding of elaborate security measures that are not truly needed. This practice is not only wasteful but it affords contractors, that already have elaborate areas or systems in place (at government expense), an unfair competitive advantage over those that do not.

PREPARED STATEMENT OF KATHLEEN A. BUCK

I. INTRODUCTION

THE PERSONNEL SECURITY PROGRAM THAT WE ARE DISCUSSING TODAY HAS ITS ROOTS IN OUR CONSTITUTIONAL FORM OF GOVERNMENT WHICH PROVIDES AMONG OTHER THINGS THAT THE EXECUTIVE HAS THE RESPONSIBILITY OF DEVELOPING AND IMPLEMENTING A PROGRAM TO PROTECT THE SECURITY OF OUR NATION. UNITED STATES CONSTITUTION, ARTICLE II, SECTION 2. IN RESPONSE TO THIS CONSTITUTIONAL DUTY, THE EXECUTIVE HAS, IN FACT, DEVELOPED AN EXTENSIVE PERSONNEL SECURITY PROGRAM. BEGINNING AS EARLY AS APRIL 27, 1953 WHEN EXECUTIVE ORDER 10450 WAS SIGNED INTO LAW BY PRESIDENT EISENHOWER, THE EXECUTIVE HAS - IN MODERN TIMES - ATTEMPTED TO FULFILL ITS MISSION OF SAFEGUARDING CLASSIFIED INFORMATION AND THUS PROTECTING THE SECURITY OF OUR NATION. AS RECENTLY AS APRIL 2, 1982, PRESIDENT REAGAN SIGNED INTO EFFECT EXECUTIVE ORDER 12356 DEALING WITH NATIONAL SECURITY INFORMATION. IN THIS

EXECUTIVE ORDER, PRESIDENT REAGAN REAFFIRMED LONGSTANDING PERSONNEL SECURITY PRACTICES BY INDICATING THAT ONLY THOSE INDIVIDUALS WHOSE ELIGIBILITY FOR OR ACCESS TO CLASSIFIED INFORMATION WAS CLEARLY CONSISTENT WITH THE NATIONAL SECURITY, AS DETERMINED BY THE HEAD OF AN AGENCY OR OTHER DESIGNATED OFFICIALS, COULD HAVE ACCESS TO THE MILITARY SECRETS OF OUR NATION. PURSUANT TO THIS GENERAL EXECUTIVE GUIDANCE, THE DEPARTMENT OF DEFENSE HAS WORKED TOWARD THE GOAL OF SAFEGUARDING CLASSIFIED INFORMATION AND ENSURING THAT ONLY THOSE INDIVIDUALS WHO ARE IN FACT CLEARLY TRUSTWORTHY, CLEARLY RELIABLE, AND CLEARLY CAPABLE OF PROTECTING THE MILITARY SECRETS OF OUR NATION GAIN ELIGIBILITY FOR OR ACCESS TO CLASSIFIED INFORMATION FOR CONTROLLED AREAS. IN DECEMBER 1979, THE DEPARTMENT IMPLEMENTED DOD 5200.2-R, THE DOD PERSONNEL SECURITY REGULATION. THIS REGULATION SETS FORTH THE BASIC GUIDANCE WITHIN THE DEPARTMENT BY WHICH THE PERSONNEL SECURITY PROGRAM IS IMPLEMENTED AND BY WHICH DETERMINATIONS REGARDING PERSONNEL SECURITY CLEARANCES AND OTHER PERSONNEL SECURITY MATTERS ARE MADE.

IN UNDERSTANDING THE ROLE OF THESE EXECUTIVE ORDERS AND THE DOD PERSONNEL SECURITY PROGRAM, IT IS IMPORTANT TO REALIZE THAT CONGRESS HAS TRADITIONALLY UNDERSTOOD THAT THE SUCCESSFUL IMPLEMENTATION OF A PERSONNEL SECURITY PROGRAM WITHIN THE EXECUTIVE BRANCH REQUIRES THAT GREAT DEFERENCE BE GIVEN TO THE EXECUTIVE AND THE EXECUTIVE AGENCIES. AS PART OF THIS RECOGNITION, CONGRESS ENACTED SECTION 7532 OF TITLE 5 OF THE U.S. CODE. (THIS PROVISION TRACES ITS HISTORY TO LAWS FIRST PASSED DURING WORLD WAR II.) IN SECTION 7532, CONGRESS HAS DECLARED THAT IN SITUATIONS IN WHICH THE HEAD OF AN AGENCY BELIEVES THAT THE INTERESTS OF NATIONAL SECURITY ARE SERVED BY THE SUMMARY SUSPENSION AND REMOVAL OF AN AGENCY EMPLOYEE, THE AGENCY HEAD MAY DO SO. MORE IMPORTANTLY, HOWEVER, THE AGENCY HEAD'S DECISION TO SUSPEND OR REMOVE AN EMPLOYEE UNDER SECTION 7532 IS FINAL AND NOT REVIEWABLE EXCEPT TO ENSURE COMPLIANCE WITH THE PROCEDURAL REQUIREMENTS SET FORTH IN THE SECTION. BY ENACTING SUCH LAWS AS 5 U.S.C. SECTION 7532 AND ITS PREDECESSORS, CONGRESS HAS GIVEN TO DOD THE NECESSARY DISCRETION TO PROTECT THE NATIONAL SECURITY AND

ITS CLASSIFIED INFORMATION. INDEED, DURING THE PAST THREE DECADES IN WHICH DOD'S PERSONNEL SECURITY PROGRAM HAS GROWN AND DEVELOPED, CONGRESS HAS RECOGNIZED THE EXECUTIVE'S LATITUDE TO DEVELOP A PERSONNEL SECURITY PROGRAM AND WORK WITHIN ITS PARAMETERS. SINCE THE LATE 1950S AND EARLY 1970S, HOWEVER, COURT DECISIONS HAVE HAD AN IMPORTANT IMPACT ON DOD'S PERSONNEL SECURITY PROGRAM.

II. CONSTITUTIONAL DUE PROCESS: JUDICIAL INQUIRIES

AS PART OF THE CONSTITUTIONAL FUNCTION OF THE JUDICIARY, FEDERAL COURTS HAVE INQUIRED INTO VARIOUS TYPES OF DOD DECISIONS TO DETERMINE WHETHER THE AGENCY HAS OVERSTEPPED THE PROPER BOUNDS OF ITS AUTHORITY OR ACTED IN VIOLATION OF THE DUE PROCESS GUARANTEED TO INDIVIDUALS UNDER THE CONSTITUTION.

FEDERAL COURTS DURING THE LATE 1960S AND EARLY 1970S INCREASINGLY HEARD CHALLENGES RAISED BY HOMOSEXUALS TO THE DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY CLEARANCE PROGRAM. THOSE CASES ESSENTIALLY INVOLVED CHALLENGES TO THE CRITERIA USED BY THE DEPARTMENT OF DEFENSE TO DETERMINE WHETHER A HOMOSEXUAL

WAS ENTITLED TO A SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION. THE COURTS, IN THESE CASES, INDICATED THAT IT WAS IMPROPER FOR THE DEPARTMENT TO REFUSE TO GRANT AN INDIVIDUAL A SECURITY CLEARANCE SIMPLY BECAUSE THE INDIVIDUAL WAS A HOMOSEXUAL. INDEED, WHILE THE COURTS RECOGNIZE THAT SUSCEPTIBILITY TO COERCION AND BLACKMAIL ARE PROPER CONSIDERATIONS FOR DOD AGENCIES THAT FUNCTION IN THE PERSONNEL SECURITY AREA, THE COURTS HAVE NEVERTHELESS HELD THAT UNLESS THE DEPARTMENT CAN DEMONSTRATE THAT A "RATIONAL NEXUS" EXISTS BETWEEN HARM TO THE NATIONAL SECURITY AND AN INDIVIDUAL'S HOMOSEXUAL ACTIVITIES, THE DENIAL OF A SECURITY CLEARANCE WILL BE DEEMED IMPROPER. IN SOME CASES (E.G. ADAMS V. LAIRD, 420 F.2D 230 (D.C. CIRCUIT 1969), CERT. DENIED, 397 U.S. 1039 (1970)), THE COURTS WERE SATISFIED THAT THE DEPARTMENT HAD MADE A SUFFICIENT SHOWING THAT A PARTICULAR HOMOSEXUAL, BECAUSE OF HIS SECRETIVE CONDUCT, WAS, IN FACT, SUSCEPTIBLE TO BLACKMAIL AND COERCION AND, THEREFORE, WAS PROPERLY DENIED A PERSONNEL SECURITY CLEARANCE AND THE CORRESPONDING ACCESS TO CLASSIFIED INFORMATION.

AS ONE EXAMPLE OF OUR CURRENT PROBLEMS, IN A CASE NOW PENDING BEFORE THE UNITED STATES DISTRICT COURT IN THE NORTHERN DISTRICT OF CALIFORNIA, A GROUP OF HOMOSEXUALS WORKING IN THE HIGH TECHNOLOGY INDUSTRY HAS SUED THE DEPARTMENT OF DEFENSE SEEKING DECLARATORY AND INJUNCTIVE RELIEF FROM THE COURT WITH REGARD TO THE DEPARTMENT'S PERSONNEL SECURITY PROGRAM. THE CASE COULD PRESENT DIFFICULTIES FOR THE DOD INDUSTRIAL SECURITY PROGRAM.

PLAINTIFFS IN THIS ACTION ARE SEEKING DECLARATORY JUDGMENT THAT THE DEFENSE DEPARTMENT'S INVESTIGATIONS OF HOMOSEXUALS TO DETERMINE SUSCEPTIBILITY TO BLACKMAIL, STABILITY OF LIFESTYLE, AND/OR PRESENCE OF CRIMINAL CONDUCT IS UNLAWFUL AND VIOLATES THEIR CONSTITUTIONAL RIGHTS. IN ADDITION, PLAINTIFFS ARE SEEKING AN INJUNCTION REQUIRING THE DIRECTOR OF THE DEFENSE INVESTIGATIVE SERVICE, THE DIRECTOR OF THE DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE, AND OTHER DEPARTMENTAL OFFICIALS TO GRANT A SECURITY CLEARANCE TO HOMOSEXUAL APPLICANTS AND TO REFRAIN FROM SUBJECTING KNOWN OR ALLEGED HOMOSEXUALS TO INVESTIGATION BASED ON

SEXUAL ORIENTATION. THE FACT THAT AN INDIVIDUAL APPLICANT OR SECURITY CLEARANCE HOLDER MAY BE A HOMOSEXUAL DOES NOT MEAN THAT THE DEPARTMENT WOULD NECESSARILY DENY THAT INDIVIDUAL A SECURITY CLEARANCE OR ACCESS TO CLASSIFIED INFORMATION. IN FACT, TWO OF THE THREE NAMED PLAINTIFFS IN HIGH TECH GAYS, ET AL. V. DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE, ET AL., CIVIL ACTION NO. C84-6078-TEH (N.D. CAL.) HAVE BEEN GRANTED SECURITY CLEARANCES. HOWEVER, INFORMATION INDICATING THAT AN INDIVIDUAL IS OR MAY BE A HOMOSEXUAL REQUIRES THAT THE DEPARTMENT FULFILL ITS CONSTITUTIONAL DUTY OF INQUIRING TO THE FULLEST POSSIBLE EXTENT WHETHER THE INDIVIDUAL - BY VIRTUE OF SECRETIVE CONDUCT OR OTHER ACTIONS INDICATING LACK OF GOOD SOUND JUDGMENT - SHOULD HAVE ACCESS TO CLASSIFIED INFORMATION. NEVERTHELESS, THE SUIT IS CONTINUING, AND THE DEPARTMENT WILL HAVE TO AWAIT THE FINAL OUTCOME TO SEE WHAT IMPACT THE COURT'S DECISION WILL HAVE ON THE DOD PERSONNEL SECURITY PROGRAM.

THE DEPARTMENT OF DEFENSE, UNDERSTANDING THAT PROCEDURAL FAIRNESS IS AN IMPORTANT PART OF THE PERSONNEL SECURITY PROGRAM, HAS ESTABLISHED A ROUTINE PROCESS THAT MEETS - AND EXCEEDS - ALL REQUIREMENTS OF PROCEDURAL DUE PROCESS BEFORE ACTION IS TAKEN TO REVOKE OR DENY A CLEARANCE TO A SECURITY CLEARANCE APPLICANT. DOD 5200.2-R, "PERSONNEL SECURITY PROGRAM," DECEMBER 1979, SECTIONS 8-200, 8-201. PURSUANT TO THIS DOD PERSONNEL SECURITY REGULATION, THE DEPARTMENT REQUIRES THAT PRIOR TO TAKING AN UNFAVORABLE PERSONNEL SECURITY DETERMINATION, THE DEPARTMENT MUST - TO THE EXTENT POSSIBLE - GIVE THE APPLICANT OR CLEARANCE HOLDER WRITTEN NOTICE OF THE PENDING ACTION, THE OPPORTUNITY TO RESPOND, AND THE OPPORTUNITY TO APPEAL ANY UNFAVORABLE DETERMINATION TO A HIGHER LEVEL WITHIN THE DEPARTMENT.

IN THE AREA OF INDUSTRIAL SECURITY, EVEN GREATER PROCEDURES ARE AFFORDED IN ACCORDANCE WITH EXECUTIVE ORDER 10865 AND THE UNITED STATES SUPREME COURT DECISION IN GREENE V. MCELROY, 360 U.S. 474 (1959). IN THE GREENE CASE, THE SUPREME COURT INDICATED THAT OUR DENYING A SECURITY CLEARANCE APPLICANT THE OPPORTUNITY TO CONFRONT ADVERSE WITNESSES AND CROSS EXAMINE SUCH WITNESSES WAS NOT AUTHORIZED BY STATUTE OR BY EXECUTIVE ORDER. THE SUPREME

COURT DID NOT DISCUSS THE VALIDITY OF A PROPERLY-AUTHORIZED PROGRAM THAT WOULD PERMIT SUCH LIMITATIONS UPON CROSS EXAMINATION AND CONFRONTATION, INSTEAD LIMITING ITS DECISION TO THE FACT THAT THE DEPARTMENT OF DEFENSE DID NOT HAVE ANY EXISTING AUTHORIZATION FOR THIS ASPECT OF ITS PROGRAM. SUBSEQUENTLY, PRESIDENT EISENHOWER SIGNED INTO EFFECT EXECUTIVE ORDER 10865, WHICH AUTHORIZED THE DEPARTMENT OF DEFENSE TO DEVELOP AND IMPLEMENT A THOROUGH, DETAILED INDUSTRIAL PERSONNEL SECURITY CLEARANCE PROGRAM.

THE ESSENCE OF THE JUDICIAL DECISIONS IN THE AREA OF PERSONNEL SECURITY HAS BEEN A JUDICIAL WILLINGNESS TO SECOND-GUESS THE EXPERT DETERMINATIONS MADE BY THE DEPARTMENT'S SECURITY PROFESSIONALS WHO ARE ENGAGED IN PERSONNEL SECURITY FUNCTIONS. THE JUDICIARY HAS, OVER THE YEARS, DEVELOPED THEIR OWN AGENDAS TO DETERMINE WHEN AND HOW TO INTERVENE IN DECISIONS MADE BY THE EXECUTIVE THAT AFFECT THE NATIONAL SECURITY. COURTS, IN SOME INSTANCES, FOCUSED ON THE ISSUE OF THE SEPARATIONS OF POWERS AND THE RIGHT OF COURTS TO INQUIRE INTO

SUCH EXECUTIVE DECISIONS. SEE, E.G., GOLDWATER V. CARTER, 444 U.S. 996, 997-98 (1979)(POWELL, J., CONCURRING); GILLIGAN V. MORGAN, 413 U.S. 1, 6-12 (1973); FLAST V. COHEN, 392 U.S. 83, 94-97 (1968); BAKER V. CARR 369 U.S. 186, 208-11, 217 (1962). OTHER COURTS HAVE SEEN THE ISSUE AS BEING ONE AKIN TO COMITY. SEE, E.G., MINDES V. SEAMAN, 453 F.2D 197, 201-202 (5TH CIR. 1971). THE THRUST OF BOTH OF THESE DOCTRINES IS SIMPLY WHETHER A FEDERAL COURT WILL BECOME EMBROILED IN THE CONSTITUTIONAL FUNCTION OF THE DEPARTMENT IN PROTECTING THE NATIONAL SECURITY. THE COURTS HAVE DISTILLED THREE MAIN ISSUES THAT GUIDE THE JUDICIARY IN DETERMINING WHETHER TO INTERVENE OR DEFER TO EXECUTIVE DECISIONMAKING. THEY ARE FIRST, WHETHER THE CONSTITUTION REQUIRES REVIEW OR INSTEAD MANDATES NON-INTERVENTION. SECOND, WHETHER JUDICIAL INTERVENTION WOULD INTRUDE UPON AREAS THAT ARE BEST LEFT TO AGENCY EXPERTISE AND DISCRETION. AND THIRD, WHETHER PRUDENTIAL CONSIDERATIONS COUNSELED AGAINST JUDICIAL INTERVENTION.

IN DETERMINING WHETHER THEY ARE AUTHORIZED TO INTERVENE OR MUST DEFER TO AGENCY DECISIONS CONCERNING PERSONNEL SECURITY CLEARANCES, THE COURTS SHOULD LOOK AT TWO SEPARATE FACTORS: (1) THE NATURE OF PLAINTIFFS' COMPLAINT, AND (2) WHETHER THE SUBJECT MATTER IS CONSTITUTIONALLY COMMITTED TO BRANCHES OF THE GOVERNMENT OTHER THAN THE JUDICIAL BRANCH. ON THE LATTER POINT, IT IS CLEAR THAT THE CONSTITUTIONAL DISTRIBUTION OF POWERS AND RESPONSIBILITY CHARGES THE EXECUTIVE, NOT THE JUDICIARY, WITH THE DUTY OF PROTECTING OUR NATIONAL SECURITY. U.S. CONSTITUTION, ARTICLE II, SECTION 2. SEE NEW YORK TIMES COMPANY V. UNITED STATES, 403 U.S. 713 729-30 (1971)(STEWART, J., CONCURRING); COLE V. YOUNG, 351 U.S. 536 (1956); GREENE V. MCELROY, 254 F.2D 944, 953-54 (D.C. CIR. 1958), REVERSED ON OTHER GROUNDS, 360 U.S. 474 (1959). THE EXECUTIVE HAS RESPONDED TO ITS CONSTITUTIONAL DUTY BY DEVELOPING A PROGRAM THAT GUARANTEES THE TRUSTWORTHINESS OF THE EXECUTIVE AGENCY EMPLOYEES, PARTICULARLY THOSE WHO WILL HAVE ACCESS TO CLASSIFIED INFORMATION. SEE EXECUTIVE ORDERS 10450, 12356. SUCCESSFUL OPERATION OF THIS PROGRAM, HOWEVER, REQUIRES

THAT THE EXECUTIVE BE GIVEN DISCRETION TO DETERMINE WHO MAY HOLD CLEARANCES, WHAT POSITIONS REQUIRE CLEARANCES TO BE HELD, AND WHEN AN EMPLOYEE MAY HAVE ACCESS TO CLASSIFIED INFORMATION. AS NOTED EARLIER, CONGRESS HAS ACCEPTED THIS GENERAL PRINCIPLE OF THE EXECUTIVE'S PROGRAM TO PROTECT NATIONAL SECURITY. SEE, E.G., 5 U.S.C. SECTION 7532.

WHILE FEDERAL COURTS HAVE INTERVENED IN AGENCY SECURITY CLEARANCE DETERMINATIONS TO ENSURE THAT CONSTITUTIONALLY PROTECTED CONDUCT HAS NOT BEEN UNREASONABLY INFRINGED UPON, SEE, E.G., CAFETERIA AND RESTAURANT WORKERS UNION V. MCELROY 367 U.S. 886 (1961); MARKS V. SCHLESINGER, 384 F.SUPP. 1373, 1776-77, (C.D. CAL. 1974), THE COURTS HAVE BEEN EQUALLY CERTAIN TO ABSTAIN FROM JUDICIAL INTERVENTION WHEN INTERNAL DEFENSE JUDGMENTS ON MATTERS AFFECTING NATIONAL SECURITY ARE AT STAKE. E.G., GILLIGAN V. MORGAN, 413 U.S. 1, 6-12 (1973)(REFUSING TO INTERVENE IN THE TRAINING, OPERATIONS, AND EQUIPPING OF THE ARMED FORCES); ORLOFF V. WILLOUGHBY, 345 U.S. 83, 93-95 (1953)(REFUSING TO INTERVENE IN MILITARY APPOINTMENTS AND DUTY ASSIGNMENTS). UNTIL 1982, THE

FEDERAL JUDICIARY WOULD ONLY INTERVENE IN A DEPARTMENT OF DEFENSE DECISION IF A PLAINTIFF RAISED A VIABLE CONSTITUTIONAL ISSUE, AND UNTIL 1982, THE FEDERAL COURTS WERE THE ONLY REAL SOURCES OF EXTERNAL INTERVENTION INTO THE PERSONNEL SECURITY FIELD. IN 1982, HOWEVER, THIS CHANGED.

III. LEGAL DEVELOPMENTS

ON APRIL 30, 1982, THE SCOPE OF JUDICIAL REVIEW OF EXECUTIVE AGENCIES' PERSONNEL SECURITY DETERMINATIONS WAS GREATLY ALTERED. THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA, IN HOSKA V. DEPARTMENT OF THE ARMY, 677 F.2D 131 (D.C. CIR. 1982), DECLARED THAT EVEN IN CASES IN WHICH NO CONSTITUTIONAL ISSUES OR CLAIMS WERE RAISED, FEDERAL COURTS WERE EMPOWERED TO DETERMINE FOR THEMSELVES WHETHER THE DEPARTMENT'S PERSONNEL SECURITY DETERMINATION WAS "ACCEPTABLE." THE COURT APPEARED TO HOLD THAT THE JUDICIARY COULD REQUIRE THAT DOD PROVE OBJECTIVELY A RATIONAL NEXUS BETWEEN ITS SECURITY CLEARANCE DECISION AND THE FACTS KNOWN TO IT CONCERNING THE CLEARANCE APPLICANT OR HOLDER. RELYING ON CASES THAT HAD NOTHING TO DO WITH NATIONAL SECURITY OR

SECURITY CLEARANCES, THE COURT CAME TO THE CONCLUSION THAT IT COULD INDEED REVIEW SECURITY CLEARANCE DETERMINATIONS TO ENSURE THAT A SO-CALLED "NEXUS" COULD BE ESTABLISHED BY THE AGENCY IN COURT. EVEN MORE ALARMINGLY, THE COURT OF APPEALS CONCLUDED THAT IT WAS POSSIBLE TO ENTER AN ORDER ACTUALLY FORCING AN AGENCY, SUCH AS THE DEPARTMENT OF DEFENSE, TO ISSUE A SECURITY CLEARANCE OR GRANT ACCESS TO CLASSIFIED INFORMATION BASED ON THE COURT'S DETERMINATION.

THE HOSKA COURT'S DECISION WAS A DEPARTURE FROM THE TRADITIONAL RESTRAINT PRACTICED BY THE FEDERAL COURTS. AS NOTED BEFORE, FEDERAL COURTS WOULD ONLY SEEK TO DETERMINE, WHEN CONSTITUTIONAL ISSUES WERE RAISED BY A PLAINTIFF, WHETHER AN AGENCY'S SECURITY CLEARANCE DETERMINATION VIOLATED PROCEDURAL DUE PROCESS OR UNDULY INFRINGED ON CONSTITUTIONALLY-PROTECTED CONDUCT. IN HOSKA, HOWEVER, THE COURT WENT FURTHER. FIRST, PLAINTIFF HOSKA DID NOT IN ANY WAY PRESENT A CONSTITUTIONAL CLAIM. THERE WAS NO INDICATION THAT THE CRITERIA RELIED UPON BY THE DEPARTMENT OF THE ARMY INFRINGED UPON HIS RIGHTS TO PRIVACY, FREE SPEECH, ASSOCIATION OR DUE PROCESS; INSTEAD, THE ARMY POINTED TO THREE SECURITY VIOLATIONS, ALLEGATIONS CONCERNING HIS PSYCHIATRIC STABILITY, AND INCIDENTS OF SEXUAL MISCONDUCT AND INDISCRETE BEHAVIOR TO ESTABLISH THE VALIDITY OF ITS DECISION TO REVOKE HOSKA'S CLEARANCE. THE COURT SUGGESTED THAT IT HAD THE POWER TO MAKE AN OBJECTIVE JUDICIAL INQUIRY INTO THE FACTS SURROUNDING THE DEPARTMENT'S SECURITY CLEARANCE DETERMINATION TO DECIDE FOR ITSELF WHETHER THE DEPARTMENT HAD ESTABLISHED A "NEXUS" BETWEEN THE KNOWN FACTS AND THE ULTIMATE PERSONNEL SECURITY DETERMINATION.

THE COURT OF APPEALS DECISION IN HOSKA, STANDING ALONE, MAY CREATE A PRECEDENT IN THE SECURITY CLEARANCE AREA, FOR THE COURT OF APPEALS SUBSTITUTED ITS JUDGMENT ON THE FACTS. DOD BELIEVES THAT AFTER HOSKA, IT IS NO LONGER SUFFICIENT FOR THE DEPARTMENT TO EXAMINE ALL KNOWN INFORMATION AND BASE A CLEARANCE DECISION ON THE STANDARD THAT ONLY THOSE WHO ARE CLEARLY TRUSTWORTHY AND WHOSE ACCESS TO CLASSIFIED IS CLEARLY CONSISTENT WITH THE NATIONAL SECURITY ARE GRANTED A CLEARANCE FOR ACCESS TO

CLASSIFIED INFORMATION. YET, THERE CAN BE NO DOUBT THAT THE PRINCIPLE OBJECTIVE OF DOD'S PERSONNEL SECURITY ADJUDICATION FUNCTION IS TO ENSURE SELECTION OF PERSONS FOR SENSITIVE POSITIONS WHOSE ACCESS TO CLASSIFIED INFORMATION IS CLEARLY CONSISTENT WITH THE NATIONAL SECURITY.

RAMIFICATIONS OF THE HOSKA DECISION ARE SERIOUS. MR. HOSKA, YOU SEE, WAS A FEDERAL CIVILIAN SERVANT WHO, AS A RESULT OF THE ARMY'S UNFAVORABLE PERSONNEL SECURITY DETERMINATION, FAILED TO MEET THE CONDITIONS OF EMPLOYMENT IN A SENSITIVE POSITION AND WAS THEREFORE REMOVED FROM FEDERAL EMPLOYMENT. MR. HOSKA HAD FIRST APPEALED THE MATTER TO THE MERIT SYSTEMS PROTECTION BOARD, THE QUASI-JUDICIAL ENTITY WHICH HEARS APPEALS FROM AGENCY ACTIONS SUCH AS REMOVALS AND REDUCTIONS. 5 U.S.C. SECTION 7512 (1-5); 7513(D). UNTIL THE HOSKA DECISION, THE BOARD HAD NEVER CHALLENGED THE DEPARTMENT'S EXPERT JUDGMENT ON A SECURITY DETERMINATION THAT LED TO A REDUCTION OR REMOVAL FROM THE SERVICE. SUBSEQUENT TO HOSKA, HOWEVER, THE BOARD HAS DETERMINED THAT THE COURT OF APPEALS IN HOSKA GAVE THE BOARD THE AUTHORITY TO INQUIRE

INTO THE MERITS OF EXECUTIVE SECURITY CLEARANCE DETERMINATIONS. THE BOARD HAS WILLINGLY ACCEPTED THIS CHALLENGE AND HAS UNDERTAKEN THE SAME TYPES OF SECURITY CLEARANCE REVIEWS IN WHICH THE HOSKA COURT ITSELF ENGAGED. THUS, NOT ONLY MUST THE DEPARTMENT SATISFY A FEDERAL COURT OF THE LEGITIMACY OF ITS SECURITY DECISIONS, NOW IT MUST ALSO DO SO BEFORE THE MERIT SYSTEMS PROTECTION BOARD, AN ADMINISTRATIVE TRIBUNAL WHICH CONGRESS CREATED SOLELY TO HEAR APPEALS FROM THE TYPES OF PERSONNEL ACTIONS SPECIFIED BY RULE, REGULATION, OR LAW. 5 U.S.C. SECTIONS 1205(A)(1); 7701(A).

BY FEDERAL REGISTER NOTICE IN DECEMBER OF LAST YEAR, HOWEVER, THE MERIT SYSTEMS PROTECTION BOARD SOLICITED AMICUS CURIAE BRIEFS ON THE ISSUE OF WHETHER THE BOARD MAY REVIEW EXECUTIVE AGENCIES' SECURITY CLEARANCE DETERMINATIONS. THE DEPARTMENT OF DEFENSE SUBMITTED SUCH A BRIEF AND I HAVE ATTACHED A COPY FOR YOUR REFERENCE. IT IS NECESSARY TO EXAMINE THE FACTS OF SOME OF THESE CASES NOW BEFORE THE BOARD.

THE RELEVANT FACTS IN THE CASES UNDER REVIEW ARE STRIKINGLY SIMILAR. IN EACH, THE APPELLANT WAS EMPLOYED IN A MILITARY OR OTHER DEFENSE FACILITY WHERE HIS JOB REQUIRED ACCESS TO INFORMATION, OBJECTS, PLACES, OR PERSONS MADE SENSITIVE BY THEIR IMPORTANCE TO THE NATIONAL SECURITY. IN TWO OF THE CASES, APPELLANTS WERE EMPLOYEES OF THE PORTSMITH (NEW HAMPSHIRE) NAVAL SHIP YARD, THE SOLE FUNCTION OF WHICH IS TO OVERHAUL AND REPAIR NUCLEAR SUBMARINES. IN ANOTHER, THE APPELLANT HELD A CRITICALLY SENSITIVE POSITION AS AN ELECTRONIC EQUIPMENT MAKER, INSTALLER, AND REPAIRER AT THE UNITED STATES ARMY EAST COAST TELECOMMUNICATION CENTER AT FORT DETRICK, MARYLAND. IN ANOTHER, THE APPELLANT WAS A WORK SUPERVISOR AT THE TRIDENT NAVAL REFIT FACILITY. IN A FIFTH CASE, THE APPELLANT WAS A SPECIALIZED CARTOGRAPHER AT THE DEFENSE MAPPING AGENCY AEROSPACE CENTER IN ST. LOUIS, MISSOURI. ALL OF THESE POSITIONS REQUIRED THAT THE EMPLOYEE/APPELLANT HOLD A SECURITY CLEARANCE, BUT EACH CLEARANCE WAS REVOKED BECAUSE OF INFORMATION WHICH CAME TO LIGHT AFTER THE EMPLOYEE INITIALLY FILLED THE POSITION. AS A RESULT, ALL OF THE

APPELLANTS FAILED TO MEET THE CONDITIONS OF EMPLOYMENT IN THEIR SENSITIVE POSITION AND THEY WERE REMOVED FROM THE SERVICE.

THE MERIT SYSTEMS PROTECTION BOARD, FOLLOWING THE LEAD OF THE COURT OF APPEALS IN HOSKA, DETERMINED THAT IT WAS ABLE TO REVIEW THE FACTS UNDERLYING THE REASONS FOR, AND THE WISDOM OF, DOD'S DECISION TO REVOKE THE SECURITY CLEARANCES. THE BOARD'S BELIEF THAT THE HOSKA DECISION EMPOWERED IT TO INQUIRE INTO THE BASIS FOR AN EXECUTIVE AGENCY'S PERSONNEL SECURITY CLEARANCE DETERMINATION IN FACT COULD AFFECT DOD'S PERSONNEL SECURITY PROGRAM; NO LONGER CAN DOD TAKE ALL AVAILABLE INFORMATION AND DETERMINE SUBJECTIVELY WHETHER - UNDER ALL THE CIRCUMSTANCES - IT IS CLEARLY CONSISTENT WITH THE NATIONAL SECURITY TO GIVE THE INDIVIDUAL ACCESS TO CLASSIFIED INFORMATION; NO LONGER CAN WE ERR ON THE SIDE OF NATIONAL SECURITY BY, IN A CLOSE CASE, CONCLUDING THAT ACCESS TO OR ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION IS NOT CLEARLY CONSISTENT WITH THE NATIONAL SECURITY. INSTEAD, IT IS POSSIBLE, BASED ON HOSKA, THAT DOD MAY NEED TO APPLY A DIFFERENT LEGAL STANDARD -- SUITABILITY RATHER THAN

TRUSTWORTHINESS. FINALLY, IN AT LEAST ONE CASE, THE BOARD HAS INDICATED THAT IT WOULD BE IN VIOLATION OF THE DRUG AND ALCOHOL REHABILITATION ACT, 42 U.S.C. SECTION 290AA ET SEQ., TO DENY A SECURITY CLEARANCE TO OR REVOKE THE EXISTING SECURITY CLEARANCE OF AN INDIVIDUAL WHO, BECAUSE OF DRUG OR ALCOHOL ACTIVITY, IS OF QUESTIONABLE TRUSTWORTHINESS UNDER THE DOD PERSONNEL SECURITY PROGRAM.

IV. DOD MANAGEMENT IMPROVEMENTS

DOD IS CHARGED NOT ONLY WITH THE FUNDAMENTAL RESPONSIBILITY OF PROTECTING THE NATIONAL SECURITY BUT ALSO WITH THE RESPONSIBILITY OF ENHANCING THE PRODUCTIVITY, ECONOMY, AND EFFICIENCY OF OUR SECURITY PROGRAMS. WE ARE MOVING AHEAD WITH MANAGEMENT IMPROVEMENTS THAT ARE NECESSARY TO ADMINISTER EFFICIENTLY THE FUNCTIONS OF THE DIRECTORATE FOR INDUSTRIAL SECURITY CLEARANCE REVIEW (DISCR).

WHEN ADVERSE INFORMATION IS DEVELOPED, THE CASE FILE IS TRANSFERRED FROM THE DEFENSE INVESTIGATIVE SERVICE TO DISCR. DOD DIRECTIVE 5220.6 ESTABLISHES THE PROCEDURES TO BE FOLLOWED WHEN

CASES ARE REFERRED TO DISCR. THE FILE IS REVIEWED TO DETERMINE WHETHER A STATEMENT OF REASONS SHOULD BE ISSUED BECAUSE IT WOULD NOT BE IN THE NATIONAL INTEREST TO GRANT A CLEARANCE. THE STATEMENT OF REASONS IS PREPARED BY A SCREENING BOARD. THE INDIVIDUAL APPLICANT MAY THEN RESPOND TO THE STATEMENT OF REASONS AND REQUEST A HEARING.

DURING THIS PAST YEAR WE HAVE AUGMENTED OUR STAFF TO REDUCE THE BACKLOG OF CASES AND MADE NUMEROUS CHANGES IN PROCEDURE TO AVOID DUPLICATION AND UNNECESSARY STEPS IN THE PROCESSING OF A CASE, AND WE HAVE INCREASED THE USE OF THE TELEPHONE TO EXPEDITE CERTAIN TYPES OF COMMUNICATIONS. IN ADDITION, INTERNAL GUIDANCE HAS BEEN ISSUED FOR PROCESSING RECOMMENDATIONS FOR SUSPENSION, APPLICANT DEFAULT, REQUESTS FOR DISCONTINUANCE OF PROCESSING, AND REQUESTS FOR REOPENING AND REINSTATEMENT. PROCEDURES HAVE BEEN ESTABLISHED TO VERIFY BY TELEPHONE THE EMPLOYMENT AND CLEARANCE STATUS OF APPLICANTS BEFORE ISSUING A STATEMENT OF REASONS.

ORIGINALLY THIS PROGRAM WAS ESTABLISHED TO PROVIDE APPLICANTS FOR CLEARANCES WITH A SIMPLE ADMINISTRATIVE HEARING

WHICH WOULD PROVIDE THE INDIVIDUAL WITH AN OPPORTUNITY TO PRESENT HIS/HER CASE TO AN OBJECTIVE HEARING OFFICER. OUR HEARING EXAMINERS ARE STRONGLY ENCOURAGED TO WRITE OPINIONS WHICH OUR APPLICANTS CAN UNDERSTAND WITHOUT THE NECESSITY TO SEEK COUNSEL. WE ARE ALSO WORKING ON TRAINING MATERIALS AND A CONFERENCE TO INSURE THE EQUAL APPLICATION OF ADJUDICATION GUIDELINES BY ALL OF OUR HEARING EXAMINERS AND ADJUDICATORS.

DURING THE LAST TWO YEARS MAJOR CHANGES HAVE BEEN MADE IN THE PROGRAM WITH THE AID OF NEW COMPUTER TECHNOLOGY. COMPUTERS INCREASE PRODUCTIVITY WITH THE ESTABLISHMENT OF NEW METHODS OF RECORDKEEPING AND ASSIGN CASES TO REDUCE TRAVEL; OF COURSE, WORD PROCESSORS ALSO FACILITATE THE WRITING OF OPINIONS AND OTHER CORRESPONDENCE. PROGRAM SPECIFICATIONS HAVE BEEN DEVELOPED TO UTILIZE THE JOINT ADJUDICATION AND CLEARANCE SYSTEM PROGRAMS USED BY THE AIR FORCE AND ARMY, TO PROVIDE A SIMPLIFIED CASE STATUS AND TRACKING SYSTEM, AND TO RECORD STATUS DATA IN THE DEFENSE CENTRAL INDEX OF INVESTIGATIONS.

WE ARE CURRENTLY IN THE PROCESS OF MERGING THE ADJUDICATION DIVISION OF THE DEFENSE INVESTIGATIVE SERVICE WITH DISCR TO EXPEDITE THE PROCESSING OF CASES AND ELIMINATE DUPLICATION OF THE ADJUDICATIVE FUNCTION. DURING THIS PAST YEAR WE HAVE BEEN ABLE TO MAKE MANY CHANGES WHICH WILL NOT ONLY EXPEDITE THESE CLEARANCE CASES BUT ASSIST THE INDIVIDUALS INVOLVED BY ELIMINATING UNNECESSARY DELAYS.

OUR PURPOSE IN IMPLEMENTING THE MANAGEMENT INITIATIVES I HAVE OUTLINED IS TO DEVELOP A PROGRAM WHICH WILL PROTECT OUR NATION'S SECRETS YET RESPOND AS QUICKLY AS POSSIBLE TO OUR CONTRACTOR COMMUNITY.

ATTACHMENT

BIBLIOGRAPHY

G. LEWY, THE FEDERAL LOYALTY - SECURITY PROGRAM: THE NEED FOR REFORM (AMERICA ENTERPRISE INSTITUTE FOR PUBLIC POLICY RESEARCH: 1983).

D. MARTIN, SCREENING FEDERAL EMPLOYEES: A NEGLECTED SECURITY PRIORITY (THE HERITAGE FOUNDATION: 1983).

R. THOMAS, "PROTECTIVE SECURITY PROCEDURES IN THE [BRITISH] PUBLIC SERVICE: SOME RECENT DEVELOPMENTS," 61 PUBLIC ADMINISTRATION 429 (WINTER 1983).

"NO RISK," TIME, JANUARY 12, 1981, AT 22.

"OUT OF THE CLOSET, IN FROM THE COLD," NEWSWEEK, JANUARY 12, 1981, AT 30.

UNITED STATES OF AMERICA
MERIT SYSTEMS PROTECTION BOARD

Bogdanowicz v. Department of the Army,)
MSPB Docket No. PH07528110587 (January 18, 1984))
)
Egan v. Department of the Navy,)
MSPB Docket No. SE07528310257 (December 22, 1983))
)
Griffin v. Defense Mapping Agency,)
MSPB Docket No. SL07528410150 (July 6, 1984))
)
Peterson v. Department of the Navy,)
MSPB Docket No. BN07528410010 (February 14, 1984))
)
Irving v. Department of the Navy,)
MSPB Docket No. BN07528410005 (September 21, 1984))
)
Skees v. Department of the Navy,)
MSPB Docket No. PH07528410257 (June 14, 1984))
)
Holtcamp v. Department of the Navy,)
MSPB Docket No. SE07528410105 (June 21, 1984))
)
Drake v. Department of the Army,)
MSPB Docket No. AT07528310851 (November 9, 1983))
)
Gibson v. Defense Mapping Agency,)
MSPB Docket No. AT07528410483 (June 26, 1984))

SECURITY CLEARANCE APPEALS

AMICUS BRIEF
OF
THE DEPARTMENT OF DEFENSE

LEONARD NIEDERLEHNER
Acting General Counsel
Department of Defense
Pentagon, Room 3E980
Washington, D.C. 20301-1600

UNITED STATES OF AMERICA
MERIT SYSTEMS PROTECTION BOARD

Bogdanowicz v. Department of the Army,)
MSPB Docket No. PH07528110587 (January 18, 1984))

Egan v. Department of the Navy,)
MSPB Docket No. SE07528310257 (December 22, 1983))

Griffin v. Defense Mapping Agency,)
MSPB Docket No. SL07528410150 (July 6, 1984))

Peterson v. Department of the Navy,)
MSPB Docket No. BN07528410010 (February 14, 1984))

Irving v. Department of the Navy,)
MSPB Docket No. BN07528410005 (September 21, 1984))

Skees v. Department of the Navy,)
MSPB Docket No. PH07528410257 (June 14, 1984))

Holtcamp v. Department of the Navy,)
MSPB Docket No. SE07528410105 (June 21, 1984))

Drake v. Department of the Army,)
MSPB Docket No. AT07528310851 (November 9, 1983))

Gibson v. Defense Mapping Agency,)
MSPB Docket No. AT07528410483 (June 26, 1984))

SECURITY CLEARANCE APPEALS

AMICUS BRIEF
OF
THE DEPARTMENT OF DEFENSE

Pursuant to the notice of opportunity to file amicus briefs published in 49 Federal Register 48623 (December 13, 1984), as amended by notice published in 50 Federal Register 2355 (January 16, 1985), the attached brief is submitted on behalf of the Department of Defense and its Components for consideration by the Merit Systems Protection Board.

LEONARD NIEDERLEHNER
Acting General Counsel
Department of Defense
Pentagon, Room 3E980
Washington, D.C. 20301-1600

TABLE OF CONTENTS

Page

ISSUES i

ANSWERS ii

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICUS* vii

ARGUMENT 1

I. THE MERIT SYSTEMS PROTECTION BOARD HAS JURISDICTION OVER REMOVAL AND REDUCTION ACTIONS, BUT IT HAS NO AUTHORITY TO REVIEW UNDERLYING PERSONNEL SECURITY CLEARANCE DETERMINATIONS. 1

A. The Board Has Jurisdiction over the Cases at Bar. 1

B. The Board Has Authority to Review the Executive Agencies' Actions in the Present Cases to Ensure Compliance with the Agencies' Own Regulations. 1

C. In the Present Cases, the Board Lacks Authority to Review the Agencies' Reasons for Revoking the Personnel Security Clearances. . . . 3

1. The Board has no independent authority to review the factual basis of an Executive Agency's security clearance determination. . . 3

2. Security clearance determinations are both legally and factually separate from an agency's decision to remove or reduce an employee for failing to meet the conditions of employment. 6

3. Congress intended that all Executive Agency security clearance determinations be beyond the review authority of the Board. 11

4. The 1982 decision of Hoska v. Department of the Army provides no authority for the Board to review Executive Agencies' security clearance determinations. 15

5. Constitutional principles and policy considerations require that the Board decline to interfere with the personnel security clearance determinations in the cases at bar. . . . 21

II. IN ANY EVENT, THE BOARD CANNOT ORDER AN EXECUTIVE AGENCY TO ISSUE OR REINSTATE A PERSONNEL SECURITY CLEARANCE OR GRANT TO AN INDIVIDUAL ACCESS TO CLASSIFIED INFORMATION OR CONTROLLED AREAS. 32

CONCLUSION 35

ISSUES

I.

Whether, in a removal or reduction case over which the Merit Systems Protection Board (Board) has jurisdiction and which is based on the affected employee's failure to meet the conditions of employment following an agency's revocation or denial of a security clearance, the Board has the authority to review the agency's stated reasons for revoking or denying the affected employee's security clearance.

II.

Whether, if the Board has such authority, the scope of its review authority extends to ordering the agency to reinstate the employee's security clearance.

III.

Whether an agency that wishes to base an action listed in 5 U.S.C. §7512 on the revocation of a security clearance may do so pursuant to 5 U.S.C. §7513 or whether, in the alternative, the exclusive basis for such an action is provided by 5 U.S.C. §7532.

IV.

Whether, if the Board's authority does not extend to ordering reinstatement of the security clearance in issue, other remedies are available to the Board.

ANSWERS

I.

In a personnel action case arising under the provisions of 5 U.S.C. §§7512-7513 over which the Board otherwise has jurisdiction, but which resulted from the affected employee's inability to meet the conditions of employment in a sensitive position following an Executive Agency's denial or revocation of the employee's security clearance, the Board is precluded from reviewing the merits of the denial or revocation decision or substituting its judgment for the expert conclusions of the agency itself.

II.

An Executive Agency faced with protecting the national security in a personnel security case has available to it several remedies, among them personnel actions provided by both 5 U.S.C. §§7512-7513 and 5 U.S.C. §7532; the latter is not an exclusive remedy, and the agency's choice to forgo employing its summary suspension and removal provisions does not thereby broaden the scope of the Board's limited review authority.

III.

While the Board may review an Executive Agency's security clearance determinations in cases such as those *sub judice* to ensure that the agency has complied with its own regulations concerning notice, opportunity to respond, and opportunity to appeal within the agency, the Board may not review the merits of the security clearance decisions themselves. If, however, the Board does review these determinations and disagrees with the agency's expert conclusions, the Board may only remand the matter to the agency for further consideration - the Board may not actually order the agency to issue or reinstate a security clearance or grant to an individual access to classified information or controlled areas.

TABLE OF AUTHORITIES

Page(s)

CASES

Adams v. Laird, 420 F.2d 230 (D.C. Cir. 1969), cert. den., 397 U.S. 1039 (1970) 12,20

American Federation of Government Employees v. Hoffman, 427 F.Supp. 1048 (N.D.Ala. 1976) 28

Atwell v. Merit Systems Protection Board, 670 F.2d 272 (D.C. Cir. 1981) 3,4

Baker v. Carr, 369 U.S. 186 (1962) 21

Barger v. Department of Justice, 10 MSPB 148 (1982) 32

Bonet v. United States Postal Service, 661 F.2d 1071 (5th Cir. 1981) 17

Broadway v. Block, 694 F.2d 979 (5th Cir. 1982) 10

Cafeteria and Restaurant Workers Union v. McElroy, 367 U.S. 886 (1961) 23

California v. Settle, 708 F.2d 1380 (9th Cir. 1983) 32

Cole v. Young, 351 U.S. 536 (1956) 6,13,22,33

Cowan v. United States, 710 F.2d 803 (Fed. Cir. 1983) . . . 3

Doe v. Hampton, 566 F.2d 265 (D.C. Cir. 1977) 17

Doe v. National Security Agency, 6 MSPB 467 (1981) 13

Dowd v. United States, 713 F.2d 720 (Fed. Cir. 1983) . . . 3

Flast v. Cohen, 392 U.S. 83 (1968) 21

Gayer v. Schlesinger, 490 F.2d 740 (D.C. Cir. 1973) 20

Gilligan v. Morgan, 413 U.S. 1 (1973) 21,24,27

Goldwater v. Carter, 444 U.S. 996 (1979) 21

Greene v. McElroy, 254 F.2d 944 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959) . . . 2,6,11,12, 22,24,31,33

Griffin v. Department of Agriculture, 2 MSPB 335 (1980) . . 10

Haig v. Agee, 453 U.S. 280 (1981) 24,34

Harrison v. McNamara, 228 F.Supp. 406 (D.Conn. 1964), aff'd per curiam, 380 U.S. 261 (1965) 13

Hondros v. United States Civil Service Commission, 720 F.2d 278 (3d Cir. 1983) 27

Hoska v. Department of the Army, 677 F.2d 131 (D.C. Cir. 1982) 15,16,17,18,19,20

Ketterer v. Federal Crop Insurance Corporation, 2 MSPB 459 (1980) 10

Latimer v. Department of the Air Force, 657 F.2d 235 (8th Cir. 1981) 4,20

Manning v. Merit Systems Protection Board, 742 F.2d 1424 (Fed. Cir. 1984) 20

Marks v. Schlesinger, 384 F.Supp. 1373 (C.D.Cal. 1974) . . 20,23

Martel v. Federal Aviation Administration, 735 F.2d 504 (Fed. Cir. 1984) 4

May v. United States Civil Service Commission, 230 F.Supp. 659 (W.D.La. 1963) 4

McClelland v. Andrus, 606 F.2d 1278 (D.C. Cir. 1979) . . . 17

McKeand v. Laird, 490 F.2d 1262 (9th Cir. 1973) 12,20

Mindel v. United States Civil Service Commission, 312 F.Supp. 485 (N.D.Cal. 1970) 17

Mindes v. Seaman, 453 F.2d 197 (5th Cir. 1971) . . 2,21,24,27

NeSmith v. Fulton, 615 F.2d 196 (5th Cir. 1980) 26

New York Times Company v. United States, 403 U.S. 713 (1971) 22

Norton v. Macy, 417 F.2d 1161 (D.C. Cir. 1969) 17

Orloff v. Willoughby, 345 U.S. 83 (1953) 24,28

Phillips v. Bergland, 586 F.2d 1007 (4th Cir. 1978) 17

Rosano v. Department of the Navy, 699 F.2d 1315 (Fed. Cir. 1983) 3

Rose v. Department of Health and Human Services, 721 F.2d 355 (Fed. Cir. 1983) 3,4

Schaffer v. Department of the Air Force, 6 MSPB 631 (1981) 28

South Corporation and Seal Fleet, Inc. v. United States, 690 F.2d 1368 (Fed. Cir. 1982) 15

Tennessee v. Dunlap, 426 U.S. 312 (1976) 6,27

Turner v. Egan, 358 F.Supp. 560 (D.Alas.), *aff'd*, 414 U.S. 1105 (1973) 28

Vitarelli v. Seaton, 359 U.S. 535 (1959) 13

Wentworth v. Laird, 348 F.Supp. 1153 (D.D.C. 1972), *aff'd sub nom. Gayer v. Schlesinger*, 490 F.2d 740 (D.C. Cir. 1973) 20

West v. Brown, 558 F.2d 757 (5th Cir. 1977), *cert. den.*, 435 U.S. 926 (1978) 28

Williams v. Department of the Army, 651 F.2d 243 (4th Cir. 1981) 3,10

Young v. Hampton, 568 F.2d 1253 (7th Cir. 1977) 17

STATUTES

5 U.S.C. §§22-1 *et seq*. (1951) 13

5 U.S.C. §701(a)(2) 27

5 U.S.C. §1205(a)(1) 1,3,9,15

5 U.S.C. §3571 14

5 U.S.C. §7312 14

5 U.S.C. §7512 1,3,4,5,8,9,11,12,13,14,15,17,18,23

5 U.S.C. §7513(d) 1,9

5 U.S.C. §7532 9,11,12,13,14,15,23

5 U.S.C. §7701(a) 1,3,9,15

5 U.S.C. §7701(c) 1,18

5 U.S.C. §7702(c) 10

5 U.S.C. §7703(b) 15

42 U.S.C. §2000e 10

UNITED STATES CONSTITUTION

Article II 22

Article III 19

EXECUTIVE ORDERS

Executive Order 10450, "Security Requirements for Government Employees," April 27, 1953. 7,23

Executive Order 12333, "United States Intelligence Activities," December 4, 1981. 7,10

Executive Order 12356, "National Security Information," April 2, 1982. 7,23

DEPARTMENTAL DIRECTIVES

DoD Directive 5200.2, "Department of Defense Personnel Security Program," December 20, 1979, 32 C.F.R. §156.1 *et seq*. 7,18

DEPARTMENTAL REGULATIONS

DoD 5200.2-R, "Department of Defense Personnel Security Program," December 1979. . . . . 2,4,7,14, 18,23,26

INTEREST OF THE AMICUS

The Department of Defense (DoD) is a Cabinet-level Executive Department charged with the responsibility of, *inter alia*, providing for the defense and security of our Nation. As part of its efforts to achieve these ends, and in accordance with Presidential directives, the Department has established a personnel security program to guarantee that only those individuals who have been determined by the Department to be trustworthy and whose access to classified information is clearly consistent with the interests of national security are granted security clearances. In fiscal year 1983 alone, the Department processed over 796,000 personnel security clearance applications.

The Department of Defense has a deep and abiding commitment to the proper and fair administration of its personnel security clearance program. Elaborate procedures have been developed within the Department to utilize the expertise and experience of its security specialists in assessing the impact that each individual clearance holder or applicant may have on the national security. The Merit Systems Protection Board, in the security clearance cases now at bar, has injected itself into this delicate process. The Department has a legitimate interest in ensuring that the Board is fully apprised of the legal and prudential limitations on - and the practical ramifications of - its actions in this area.

ARGUMENT

I. THE MERIT SYSTEMS PROTECTION BOARD HAS JURISDICTION OVER REMOVAL AND REDUCTION ACTIONS, BUT IT HAS NO AUTHORITY TO REVIEW THE UNDERLYING PERSONNEL SECURITY CLEARANCE DETERMINATIONS.

A. The Board Has Jurisdiction over the Cases at Bar.

The Merit Systems Protection Board ("Board") is empowered to hear appeals from an agency's removal of an employee from the service or its reduction of an employee in grade or pay. 5 U.S.C. §§1205(a)(1), 7512(1),(3),(4), 7513(d), 7701(a). Because such actions were taken in the cases at bar, the Board does have jurisdiction to hear these cases.

B. The Board Has Authority to Review the Executive Agencies' Actions in the Present Cases to Ensure Compliance with the Agencies' Own Regulations.

Separate from the issue of the Board's jurisdiction in the present cases is the question of the scope of the Board's review authority. For example, the Board is empowered to review an agency's removal or reduction action to ensure that the agency complied with its own procedural regulations. See, e.g., 5 U.S.C. §§7512, 7701(c)(2)(A). Likewise, where a removal or reduction results from an employee's failure to meet the conditions of his or her employment in a sensitive position requiring a clearance - following the Executive Agency's security clearance revocation or denial determination - the Board may even review the security clearance determination to ensure once again that the agency complied with its own procedural regulations to produce a facially-valid clearance determination. See Greene v. McElroy, 254 F.2d 944, 953 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959). See also Mindes v. Seaman, 453 F.2d 197, 201 (5th Cir. 1971). See generally DoD 5200.2-R, "Department of Defense Personnel Security Program," December 1979, Chapter VIII (requiring notice, an opportunity to respond, and an opportunity to appeal to a higher level within the Department before DoD takes final action to revoke a personnel security clearance, nonselect an applicant for a sensitive position, or reassign an employee to a position of lesser sensitivity). This does not mean, however, that the Board has the authority to review the factual basis for or the wisdom of the agency's actual decision to revoke or deny the personnel security clearance:

> A direct Government employee normally has procedural rights conferred by Congress, which the courts will protect. . . . But even in the case of a Government employee the courts will not inquire into the merits of a dismissal [following the loss of a security clearance]: they will inquire whether required procedures have been observed, or an applicable statute violated, but they will not - for example - attempt to determine whether an employee is or is not a "security risk" or is "untrustworthy."

Greene v. McElroy, supra, at 953.

C. In the Present Cases, the Board Lacks Authority to Review the Agencies' Reasons for Revoking the Personnel Security Clearances.

1. The Board has no independent authority to review the factual basis of an Executive Agency's security clearance determination.

In a security clearance revocation or denial case which presents no otherwise-reviewable action to the Board, there is no jurisdiction or authority for the Board to review the factual basis for or the wisdom of the Executive Agency's security clearance determination. The Merit Systems Protection Board, as an administrative tribunal created by Congress, has only that jurisdiction specifically granted to it by the statutes empowering it to act. Cowan v. United States, 710 F.2d 803, 805 (Fed. Cir. 1983); Rosano v. Department of the Navy, 699 F.2d 1315, 1318-20 (Fed. Cir. 1983); Atwell v. Merit Systems Protection Board, 670 F.2d 272, 280 (D.C. Cir. 1981). The jurisdiction of the Board is not inherent, nor can it be implied, Dowd v. United States, 713 F.2d 720, 722 (Fed. Cir. 1983), and jurisdiction exists to hear appeals only from the types of actions specifically enumerated by "law, rule or regulation." 5 U.S.C. §§1205(a)(1), 7701(a); Rose v. Department of Health and Human Services, 721 F.2d 355, 356 (Fed. Cir. 1983); Williams v. Department of the Army, 651 F.2d 243, 244 (4th Cir. 1981).

In a case in which no Section 7512 action arises from an agency's revocation or denial of a personnel security clearance, the affected employee is unable to obtain the Board's review, for he or she cannot meet the requisite burden of establishing that the security clearance determination itself falls within one of the narrow categories of Congress' limited grant of jurisdiction to the Board. See Martel v. Federal Aviation Administration, 735 F.2d 504, 506 (Fed. Cir. 1984). First, there are no rules or regulations that grant the Board the authority to review the merits of an Executive Agency's actual security clearance determinations. On the contrary, existing federal regulations make the agency's determination final. E.g., DoD 5200.2-R, supra, at ¶¶8-102, 8-103, 8-200, 8-201 (final determination is made by the appropriate DoD official after procedural benefits have been afforded). Moreover, no "law" vests such review authority in the Board. See 5 U.S.C. §§7512(1)-(5) (narrowly defining by statute the reviewable personnel actions to include only removal from employment, suspension for more than 14 days, reduction in grade, reduction in pay, and furlough of 30 days or less), 7513(d). See also Rose v. Department of Health and Human Services, supra, at 357 (AWOL determination is not a Section 7512(2) "suspension," so the Board was without authority to review plaintiff's challenge); Atwell v. Merit Systems Protection Board, supra, at 282-86 (a downward reclassification leading to a downgrade is not a Section 7512 "reduction," so review authority absent); Latimer v. Department of the Air Force, 657 F.2d 235, 237 (8th Cir. 1981)(no basis for review because only a non-promotion was involved); May v. United States Civil Service

Commission, 230 F.Supp. 659, 660 (W.D.La. 1963)(no authority for the Board to review an agency's administrative orders for plaintiff to report for a fitness for duty examination and to report to his supervisor to discuss work performance, notwithstanding that the plaintiff's refusal to do as ordered resulted in his removal from the service).

From the indisputable premise that an Executive Agency's personnel security clearance determinations, standing alone, are not reviewable by the Board, the issue now before the Board is more clearly stated as follows:

> Whether, in cases in which Section 7512 actions do follow from Executive Agencies' security clearance determinations because of the affected employees' inability to meet the conditions of their employment (that is, their failure to retain security clearances as required by the sensitivity of their positions), any rule, regulation, or law affirmatively enlarges the limited authority of the Board to include the power to review the otherwise-unreviewable factual bases for the agencies' decisions to revoke or deny the personnel security clearances.

The answer is that there is no such affirmative enlargement of the Board's authority and that such review is improper.

2. Security clearance determinations are both legally and factually separate from an agency's decision to remove or reduce an employee for failing to meet the conditions of employment.

In order to understand the limits on the Board's review authority in removal or reduction cases such as those now before the Board, it is necessary to realize that the decision to revoke or deny a clearance is a separate matter - both legally and factually - from the later action, if necessary, to remove an employee from the service or reduce his or her grade or pay because of a failure to meet the conditions of employment. See Tennessee v. Dunlap, 426 U.S. 312, 315-16 (1976)(state National Guard determination not to permit a member to reenlist was distinct from the statutory decision to remove him from federal civilian employment because he was no longer a member of the Guard as required by the conditions of his employment).

On the one hand, a security clearance revocation or denial is done to protect national security. See, e.g., Cole v. Young, 351 U.S. 536, 542, 546 (1956); Greene v. McElroy, 254 F.2d 944, 954 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959). The President, pursuant to his constitutional duty of protecting the national security, see part I.C.5., infra, has fashioned Executive Orders to guide the Executive Agencies in determining whether to issue a security clearance, revoke a clearance, designate a position as sensitive and thus as requiring a clearance, or grant an employee access to classified information. E.g., Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953; Executive Order 12333, "United States Intelligence Activities," December 4, 1981, at §1-11(h) (requiring the Secretary of Defense to protect the security of DoD activities, information and personnel "by appropriate means"); Executive Order 12356, "National Security Information," April 2, 1982, at §§4.1(a) (in order to safeguard national security information, only those individuals determined to be trustworthy by the head of an agency or by designated officials can have or be eligible for access to classified materials), 4.2, 5.3. The Department of Defense has taken this general guidance and implemented an extensive personnel security program. DoD Directive 5200.2, "Department of Defense Personnel Security Program," December 20, 1979, at §C.1., 32 C.F.R. §156.3(a) (clearances are granted and continued only if "clearly consistent with the interests of national security"); DoD 5200.2-R, supra, at ¶¶2-101, 2-200, 2-500, 3-102, 5-101, 6-100, 6-102, 7-100, 7-102, 9-100, Appendices F and I (detailing who may issue clearances, who may grant access to classified information, who may designate a position as sensitive, who may determine which position functions require access to classified information, and how information concerning a security clearance holder or applicant will be analyzed).

On the other hand, a removal or reduction action arises in a case such as the ones at bar because the employee's position, job requirements, or the nature or mission of the agency itself necessitates such action upon the employee's failure to meet the conditions of employment - that is, to obtain or retain a personnel security clearance in a position designated as sensitive and thus requiring such clearance as a prerequisite to employment or continued employment. As an illustration, the Department of Energy may revoke the existing personnel security clearance of one of its employees, but no reduction or removal action will occur if the Department is able to find alternate employment for the individual in a comparable, nonsensitive position. In the latter case, the Board clearly has no jurisdiction or authority to review the wisdom of or the factual basis for the actual security clearance determination. See part I.C.1., supra.

The distinction between a security clearance determination itself and a Section 7512 action which occurs as the result of a failure to meet conditions of employment becomes even more apparent when the foregoing illustration is contrasted with the hypothetical example of an employee in the Defense Intelligence Agency (DIA) who loses his or her clearance. While both the DIA employee and the Department of Energy employee would have had their existing clearances revoked because of a determination by the respective agency officials that continued access to classified information was not clearly consistent with the national security, the DIA employee may ultimately be removed from the Agency if no comparable, nonsensitive positions exist within DIA.[1] If removal does occur, the Board should ensure that DIA complied with applicable DIA and DoD regulations relating to notice, opportunity to respond, and opportunity to appeal to a higher level within the Department prior to its final action on the clearance; that the clearance was in fact revoked; and that the Agency again complied with applicable procedural regulations before removing the employee. Nevertheless, there is no rule, regulation, or law that affirmatively empowers the Board to review the merits of the final revocation decision by DIA - a fact that remains true notwithstanding the fortuitous fact that no comparable employment existed within DIA to forestall the removal action. Board review of the factual basis for the security clearance determination in our hypothetical DIA case would, as a legal matter, be inconsistent with and contrary to the limited nature of the Congressional "charter" granted to the Board, 5 U.S.C. §§1205(a)(1), 7512, 7513(d), 7701(a), and, as a practical matter, would create the illogical and unintended situation of the Board's being precluded from reviewing the security clearance determination of, in our illustration, the Energy Department, while being able to challenge and disregard the identical determination made by senior DIA officials who had utilized the experience and expertise of an agency (such as the

---

[1] This hypothetical assumes that the agency chooses to proceed through routine security revocation channels rather than invoking the provisions of 5 U.S.C. §7532. See notes 3 and 5, infra.

Defense Intelligence Agency) which performs a highly specialized and critically sensitive intelligence mission.[2] *See* E.O. 12333, *supra*, at §1.12(a). The Board's reviewing the expert judgment of the DIA - or any Executive Agency - for its security clearance determinations necessarily injects the Board into the inviolable process of protecting the national security by forcing it to determine who shall have access to military secrets, what job positions can be designated as sensitive, and what missions the Executive may prescribe for its agencies and employees. This the Board cannot, and must not, do:

---

[2] Congress, facing similarly difficult choices in the past, has had to balance important - albeit competing - interests in order to achieve a proper resolution. *E.g.*, 5 U.S.C. §7702(a)(1)(A) (balancing the interest of remedying discriminatory federal employment practices against the interest of establishing workable parameters for the Board, Congress made the Board statutorily unable to review allegations of discrimination when the claimed discrimination did not result in an action that is otherwise appealable to the Board); 42 U.S.C. §2000e-2(g) (balancing the same interest of ending discriminatory employment practices against the interest of national security, Congress determined that it is not an "unlawful employment practice" to take or fail to take certain employment actions when the employee concerned fails or ceases to fulfill any requirement that is imposed in the interest of the national security of the United States under any Executive security program). So, too, in deciding whether to grant the Board the authority to review the merits of Executive Agencies' personnel security clearance determinations, Congress - being historically aware of the competing interests at stake - deliberately chose not to include such personnel security determinations within the scope of the Board's review powers, regardless of whether an otherwise appealable action was also presented to the Board for resolution. *See Williams v. Department of the Army*, 651 F.2d 243 (4th Cir. 1981); *Broadway v. Block*, 694 F.2d 979 (5th Cir. 1982); *Ketterer v. Federal Crop Insurance Corporation*, 2 MSPB 459 (1980); *Griffin v. Department of Agriculture*, 2 MSPB 335 (1980).

> [F]or a court to hear de novo the evidence as to [an individual's] fitness to be assigned to particular kind of confidential work [or for access to classified information] would be a bootless task, involving judgments remote from the experience and competence of the judiciary. Indeed, any meaningful judgment in such matters must rest on considerations of policy, and decisions as to comparative risks, appropriate only to the executive branch of the Government. . . .

Greene v. McElroy, 254 F.2d 944, 953, 954 (D.C. Cir. 1958), *rev'd on other grounds*, 360 U.S. 474 (1959). *See* part I.C.5., *infra*.

3. Congress intended that all Executive Agency security clearance determinations be beyond the review authority of the Board.

Congress, in addition to evincing an intent to leave the matter of security clearance determinations to agency expertise and discretion by its not challenging the Executive personnel security program that has been developed over the past three decades, has also specifically removed from the Board's review authority the power to hear or adjudicate suspension and removal actions taken by Executive Agencies pursuant to the provisions of 5 U.S.C. § 532.[3] 5 U.S.C. §7512(A). The framework of Section 7532, when considered in conjunction with the lack of affirmative authority for the Board to review personnel security clearance determinations *per se*, *see* 5 U.S.C. §7512(1)-(5), manifests the intent of Congress to make such security clearance determinations unreviewable by the Board.

---

[3] Action taken pursuant to Section 7532 is a nonexclusive alternative available to an Executive Agency to safeguard classified information and protect national security. *See* note 5, *infra*.

While neither Section 7512 nor Section 7532 specifically mentions the reviewability of Executive security clearance determinations that do not also result in Section 7532 suspensions or removals, the intent of Congress is nevertheless clear. First, had Congress desired to extend affirmatively the Board's authority to include the power to review the reasons for Executive Agencies' personnel security clearance determinations in non-Section 7532 cases, it could certainly have done so; however, its purposeful decision to the contrary, made at a time when even courts were declining to substitute their judgment for agencies' security clearance determinations, reveals that Congress never envisioned such review by the Board.[4] See, e.g., Adams v. Laird, 420 F.2d 230, 239-40 (D.C. Cir. 1969), cert. den., 397 U.S. 1039 (1970); Greene v. McElroy, 254 F.2d 944, 953-54 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959); McKeand v. Laird, 490 F.2d 1262, 1263-64 (9th Cir. 1973).

Secondly, action taken pursuant to Section 7532 is one remedy - albeit a harsh and drastic one - made available by Congress in order to enable the Executive to protect national security.[5] Thus, and in the sole discretion of the head of an agency, an agency may suspend an employee without pay, examine the pertinent allegations, apply the enumerated procedural privileges, and - if necessary - remove the suspended employee from the service. 5 U.S.C. §7532(a). The decision of the agency head is final, 5 U.S.C. §§7512(A), 7532(b), and strict limitations upon reinstatement and reemployment follow. 5 U.S.C. §§3571, 7312. It would be anomalous for Congress to have intended to allow a Section 7532 suspension of an employee without pay and his or her summary removal to be unreviewable by the Board while permitting the Board to review an agency's decision - based on the same national security concerns - to take the less harsh measures of (1) allowing the employee to continue to work and draw pay while the agency investigates the matter; (2) affording the employee full procedural process within the agency prior to its deciding whether to revoke the clearance; and finally, if a revocation occurs, (3) attempting to find alternate, comparable employment for the individual in a nonsensitive position. While it may be procedurally easier to rely on the nonreviewable operation of Section 7532 to take action against an employee in the interests of national security, Executive Agencies (such as the Department of Defense) have relegated the use of Section 7532 to those cases involving, for example, allegations of espionage or subversion.[6] For the Board to draw a distinction between a Section 7532 removal and a "routine" security clearance decision that is followed by, at worst, a Section 7512 removal or reduction is to penalize Executive Agencies for giving their employees the benefit of the doubt (when possible) and for trying to mitigate the effect of the loss of a clearance. Congress could have never intended such an incongruous result.

---

[4] See note 2, supra.

---

[5] The Board has, in the past, held that because an Executive Agency could perhaps have utilized a Section 7532 summary removal but chose not to, full Board review of the agency's actual security clearance determination was appropriate. *E.g.*, *Doe v. National Security Agency*, 6 MSPB 467, 470 n.3 (1981)(clearance revocation followed by a Section 7512 removal was deemed properly subjected to full review by the Board). The Board now seeks guidance on whether the remedy provided by 5 U.S.C. §7532 is the exclusive relief available to Executive Agencies in personnel security cases that involve civil service employees.

First, there is nothing in the history of Section 7532 or its predecessor statutes, *see*, *e.g.*, 5 U.S.C. §§22-1 *et seq.* (1951), to indicate that this provision was intended by Congress to be the sole and exclusive remedy available to an agency to deal with civil servants in or seeking sensitive positions. *See Vitarelli v. Seaton*, 359 U.S. 535, 539-40 (1959); *Harrison v. McNamara*, 228 F.Supp. 406, 407, 408 (D.Conn. 1964), *aff'd per curiam*, 380 U.S. 261 (1965). Indeed, because only employees *already* in sensitive positions may be affected by Section 7532, *Cole v. Young*, 351 U.S. 536, 543, 546, 550-51 (1956), and because routine security clearance application *denials* would thus not be encompassed, it is apparent that Section 7532 does not preempt the Executive's existing personnel security program. The very language of Section 7532 reveals the permissive nature of its invocation: the head of an agency "*may* suspend without pay" and "*may* remove" an employee when the agency head considers or determines that "such action" is advisable in the interests of our national security. 5 U.S.C. §7532(a),(b) (emphasis added).

Finally, because of the drastic nature of a Section 7532 action, *see* text *infra*, it is apparent that Congress provided Section 7532 as the "ultimate weapon" - but by no means the only weapon - in an Executive Agency's arsenal for protecting the national security. Any conclusion that the Board is authorized to review the factual basis for an agency's security clearance determination simply because the agency chose not to proceed under Section 7532 is plainly without legal or historical justification. Not only would such a position be contrary to the permissive nature of Section 7532, but it would also force - with dire consequences - Executive Agencies to choose between the Scylla of the Board's imprecise review of security clearance determinations and the Charybdis of the agencies' foregoing any attempts to mitigate the effect of the loss of a clearance. *See* text *infra*. Congress never intended such a Hobson's choice.

---

[6] Current Department of Defense guidelines prescribe that DoD civilian employees shall not be removed from employment under the provisions of the DoD personnel security program - including the utilization of Section 7532 - if removal can be effected under OPM regulations or administrative (i.e., nonsecurity) regulations of the Military Departments. DoD 5200.2-R, supra, at ¶¶8-103, 8-202.

4. The 1982 decision of Hoska v. Department of the Army provides no authority for the Board to review Executive Agencies' security clearance determinations.

Since 1982, the Board has relied upon the decision of the United States Court of Appeals for the District of Columbia Circuit in Hoska v. Department of the Army, 677 F.2d 131 (D.C. Cir. 1982), as the basis for its authority to review the merits of agency security clearance determinations that cause a Section 7512 action to be taken because of the affected employee's failure to meet the conditions of employment. However, and for a variety of reasons, Hoska does not provide the requisite "law" or "rule" upon which the Board's review authority must rest. See 5 U.S.C. §§1205(a)(1), 7701(a). As the following discussion reveals, the Board must decline to rely on the holding in Hoska as a basis for asserting its review authority over the security clearance determinations in the present cases. See 5 U.S.C. §7703(b). See also South Corporation and Seal Fleet, Inc. v. United States, 690 F.2d 1368, 1370 & n.2 (Fed. Cir. 1982).

First, the Hoska court erroneously believed that the parties had conceded that if the Army had improperly revoked Mr. Hoska's clearance, then his removal from the service was also improper. 677 F.2d at 136. In fact, no such concession was ever made by the Department of the Army. More importantly, however, while the Hoska court noted that the Board had declined to challenge the propriety of the Army's actual clearance revocation decision, id. at 135, 136 & n.6, the court never held that the Board should - or even had the authority to - inquire into the merits of such security determinations. Thus, even the Hoska decision itself does not provide a basis for such review by the Board. See text accompanying note 8, infra.

Secondly, the Hoska court's holding that a federal court could substitute its judgment for an Executive Agency's in a security clearance matter was based on the court's reliance on two separate lines of cases: the "nexus" cases (supporting its conclusion that the Government must demonstrate a nexus between the plaintiff's conduct and the security clearance determination) and the "security clearance" cases (supporting its conclusion that security clearance determinations are themselves reviewable by a court). Both lines of cases were inapposite to the facts of Hoska and thus make that decision of no real value to the Board.

The "nexus" cases cited by the *Hoska* court do in fact require an agency to prove a rational connection between the Section 7512 personnel action it has taken and the agency's articulated reasons for it.[7] 677 F.2d at 136-37. However, none of these cases presented issues of national security or removals following unfavorable - albeit nonpunitive - security clearance decisions. *McClelland v. Andrus*, 606 F.2d 1278 (D.C. Cir. 1979)(park ranger); *Doe v. Hampton*, 566 F.2d 265 (D.C. Cir. 1977)(clerk-typist with the Bureau of Engraving and Printing); *Norton v. Macy*, 417 F.2d 1161 (D.C. Cir. 1969)(budget analyst with NASA); *Phillips v. Bergland*, 586 F.2d 1007 (4th Cir. 1978) (engineer with the Department of Agriculture's Forest Service); *Bonet v. United States Postal Service*, 661 F.2d 1071 (5th Cir. 1981)(manager of a post office branch station); *Young v. Hampton*, 568 F.2d 1253 (7th Cir. 1977)(Army employee; no question of reliability or trustworthiness was raised); *Mindel v. United States Civil Service Commission*, 312 F.Supp. 485 (N.D.Cal. 1970) (post office clerk). These cases arose because the Board must, by statute, review for a nexus between an agency's removal or reduction of an employee and the purported reasons for the

---

[7] In the cases *sub judice*, the agencies demonstrated this nexus by showing that removal furthered the efficiency of the service because of the affected employees' failure to meet the conditions of continued employment. Moreover, while an Executive Agency may require an internal, *subjective* determination of whether - based on all known facts - to issue or revoke a security clearance, *see Hoska v. Department of the Army*, 677 F.2d at 138 n.11, this does not mean that the agency must *objectively* demonstrate a connection between those facts and its ultimate security decision to the Board or a court before the security clearance determination has full and final effect. *See* part I.C.5.b., *infra*.

Section 7512 action itself. *See* 5 U.S.C. §7701(c)(1)(B),(2)(C). Thus, because the "nexus" cases are limited by their facts to Section 7512 actions that were based on misconduct adversely affecting the efficiency of the service, these decisions were as inapplicable to the facts of *Hoska* as they are to the cases now before the Board. Section 7512 actions in cases such as those cited in *Hoska* result from an agency's broad assessment that the ability of an employee *to do his or her specific job* has been adversely affected by past misconduct. Such cases involve concepts that are a far cry from the constitutional principles governing security clearance determinations and, thus, the cases now before the Board - which turn on the far more stringent standard of assessing not the "efficiency of the service" but rather the future *trustworthiness* of the individual in terms of the likelihood of his or her *preserving the national security*. *See* DoD Directive 5200.2, *supra*, at §C.1., 32 C.F.R. §156.3(a); DoD 5200.2-R, *supra*, at ¶¶2-101, 2-200, 6-100, 9-100, Appendix I (after due consideration of all aspects of the information concerning the individual, a security clearance is issued only upon a determination that access to classified information is "clearly consistent with the interests of national security"). *See also* DoD Directive 5200.2, *supra*, at §D.2.a.,c., 32 C.F.R. §156.4(b)(1),(3); DoD 5200.2-R, *supra*, at ¶11-101b. (the General Counsel of the Department of Defense is required to ensure that the DoD personnel security program is administered consistently with law and in a manner that fully protects the rights of individual employees; this duty can be fulfilled only if the General Counsel, and a fortiori the Board, distinguishes between routine removals that "promote the efficiency of the service" and security clearance determinations that safeguard the national security).

Just as the Hoska court's use of the "nexus" cases as precedent was erroneous, the court's reliance on the "security clearance" cases was equally misplaced. 677 F.2d at 137-38. The court in Hoska was again correct that federal courts may review the criteria used by an agency to make a security clearance determination - and even the facts surrounding the clearance determination itself - to ensure that a determination is not arbitrary or capricious, but the court failed to recognize that such judicial intervention is preconditioned on the existence of a viable constitutional challenge to the agency's criteria or the actual clearance decision. A federal court, being vested with jurisdiction to try cases and controversies arising from the Constitution, U.S. Const., Art. III, §2, may indeed be able to review an agency's security clearance determination to ensure that an individual's rights of, for example, due process and privacy are not unduly infringed upon by the agency's application of its clearance standards to applicants for or holders of such clearances.[8] See, e.g., Adams v. Laird, 420 F.2d 230, 239 n.7, 240 (D.C. Cir. 1969), cert. den., 397 U.S. 1039 (1970)(homosexual's clearance was properly revoked because his secretive conduct made him susceptible to blackmail or coercion); McKeand v. Laird, 490 F.2d 1262, 1263-64 (9th Cir. 1973)(same). In fact, all of the "security clearance" cases that were relied upon by the Hoska court involved homosexual employees of defense contractors and their constitutional challenges to the DoD industrial personnel security program. Gayer v. Schlesinger, 490 F.2d 740 (D.C. Cir. 1973); McKeand v. Laird, 490 F.2d 1262 (9th Cir. 1973); Marks v. Schlesinger, 384 F.Supp. 1373 (C.D.Cal. 1974); Wentworth v. Laird, 348 F.Supp. 1153 (D.D.C. 1972), aff'd sub nom. Gayer v. Schlesinger, 490 F.2d 740 (D.C. Cir. 1973). In any event, and like the cases now before the Board, Hoska did not involve a constitutional challenge to the adjudicative standards of the Department of Defense or the security clearance determination that was reached. As a result, the "security clearance" cases that formed so crucial a part of the rationale for the Hoska decision were simply inapplicable.

---

[8] The Board, as an administrative tribunal with extremely limited jurisdiction and no constitutionally sanctioned charter, cannot itself enforce constitutional claims, see Manning v. Merit Systems Protection Board, 742 F.2d 1424, 1429 (Fed. Cir. 1984), and the fact that a federal court - in some circumstances - may be able to review certain aspects of an Executive Agency's personnel security program does not mean that the Board has the authority to do likewise. See Latimer v. Department of the Air Force, 657 F.2d 235, 237 n.2 (8th Cir. 1981). Thus, the Board must decline to determine itself the constitutionality of Executive Agencies' clearance decisions or security policies. The cases at bar, of course, present no actual constitutional issues, so the present review by the Board must clearly be circumscribed.

5. Constitutional principles and policy considerations require that the Board decline to interfere with the personnel security clearance determinations in the cases at bar.

As part of our constitutional heritage, the judiciary has developed guidelines to determine when - and how - to intervene in Executive decisions that affect, for example, the national security.[9] Whether framed in terms of separation of powers, *see* *Goldwater v. Carter*, 444 U.S. 996, 997-98 (1979)(Powell, J., concurring); *Gilligan v. Morgan*, 413 U.S. 1, 6-12 (1973); *Flast v. Cohen*, 392 U.S. 83, 94-97 (1968); *Baker v. Carr*, 369 U.S. 186, 208-11, 217 (1962), or as a matter akin to comity, *see* *Mindes v. Seaman*, 453 F.2d 197, 201-202 (5th Cir. 1971), the essence of these principles may be distilled into three main issues:

---

[9] Although the Board may technically be part of the Executive Branch, the nature of its sole function as a quasi-judicial entity - especially when compared to the national security function performed by Executive Agencies such as the Department of Defense - demonstrates the value of utilizing the framework developed by the courts on the issue of judicial restraint in matters affecting the national security.

(1) Wherein lies the constitutional mandate: for review or for judicial nonintervention?

(2) Would judicial intervention intrude upon areas that are best left to agency expertise and discretion?

(3) Do prudential considerations counsel against judicial interference?

a. Constitutional considerations.

The "constitutional mandate" is determined by examining two separate factors: (1) the nature of plaintiffs' complaint and (2) whether the subject matter involved (here, security clearance determinations) is constitutionally committed to branches of the Government other than the judicial. On this latter point, the constitutional distribution of powers and responsibilities charges the Executive - not the Judiciary or a quasi-judicial entity such as the Board - with the duty of protecting our national security. U.S. Const., Art. II, §2. See New York Times Company v. United States, 403 U.S. 713, 729-30 (1971)(Stewart, J., concurring); Cole v. Young, 351 U.S. 536 (1956). See also Greene v. McElroy, 254 F.2d 944, 953-54 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959)(control of classified information rests solely with the Executive). The Executive has responded to this duty by, inter alia, developing a program that ensures the trustworthiness of Executive agency employees, see E.O. 10450, supra, particularly those who will have access to classified information. See E.O. 12356, supra. Successful operation of this personnel security program requires that the Executive be given full discretion to determine (1) who may hold clearances, (2) what positions require clearances to be held, and (3) when an employee may have access to classified information. See E.O. 12356, supra, at §§4.1, 4.2, 5.3. See also DoD 5200.2-R, supra, at ¶¶2-500, 3-102, 5-101, 7-100, 7-101, 7-102, Appendix F (specifying the DoD officials and commanders who may issue clearances, grant access to classified information, designate positions as sensitive, and determine what position functions require access to classified information). Congress has accepted this aspect of the Executive's program to protect national security. See, e.g., 5 U.S.C. §§7512(A), 7532. While federal courts[10] may be able to review an agency's security clearance determination to ensure that constitutionally protected conduct has not been unreasonably infringed upon, e.g., Cafeteria and Restaurant Workers Union v. McElroy, 367 U.S. 886, 898 (1961) (Navy withdrew worker's security badge and barred her from the base); Marks v. Schlesinger, 384 F.Supp. 1373, 1376-77 (C.D.Cal. 1974)(revocation of the industrial security clearance of a homosexual employee of a defense contractor), the courts have been equally certain to abstain from judicial intervention when internal defense judgments on matters affecting national security are at stake. E.g., Gilligan v. Morgan, 413 U.S. 1, 10-11, 12 (1973)(refusing to intervene in the training, operations, and equipping of the Armed Forces); Orloff v. Willoughby, 345 U.S. 83, 93-95 (1953)(refusing to intervene in military appointments and duty assignments). See Haig v. Agee, 453 U.S. 280, 292 (1981)("matters intimately related to . . . national defense are rarely proper subjects for judicial intervention").

---

[10] See note 8, supra.

As to the nature of the claims now before the Board, the plaintiffs do not - and are not able - to demonstrate a violation of their constitutional rights,[11] nor do they even allege that the Military Departments or Defense Agencies failed to comply with their own regulations. Balancing this against the constitutional duty that is at stake and a proper respect for the efficient functioning of the Executive Branch in its role of protecting the security of the Nation, the Board must decline to question the factual bases for or the wisdom of the agencies' security clearance determinations. The constitutional mandate prescribes such noninterference in these cases. See Mindes v. Seaman, supra.

---

[11] See note 8, supra.

b. Agency expertise.

Expertise is an invaluable part of any adjudication process, and the Board has its expertise as a result of adjudicating numerous cases involving federal personnel law, merit principles, and the "efficiency of the service." Security clearance determinations, however, require a vastly different type of expertise; in such determinations, the application of the appropriate standard (that eligibility and access must be "clearly consistent with the interests of national security") to the available information concerning a clearance holder or applicant is a unique task. The Board's extending the scope of its review to include an inquiry into the reasons for an agency's security clearance determination would require the Board to move far beyond the area of its expertise and into areas involving extensive agency specialization and discretion:

> The standard which must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.
>
> The principle objective of the [Department of Defense] personnel security adjudicative function, consequently, is to assure selection of persons for sensitive positions who meet this standard. The adjudi-

> cation process involves the effort to assess the probability of future behavior which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, *taking into consideration prior experience with similar cases*, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. *It is invariably a subjective determination*, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.
>
> Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. *It involves neither the judgement [sic] of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility which could, if abused, have unacceptable consequences for the national security*.
>
> While equity demands optimal uniformity in evaluating individual cases, assuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, *and prior experience in similar cases*. All information of record, both favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness, and overall significance. *In all adjudications the protection of the national security shall be the paramount determinant*.

DoD 5200.2-R, *supra*, at ¶6-100 (emphasis added).

Courts have recognized that a key to the doctrine of nonreviewability of Executive decisions is a wise unwillingness by the judiciary to second-guess agency judgments on matters, such as national security, that require the utilization of an agency's experience and expertise.[12] *See*, *e.g.*, *Mindes v. Seaman*, *supra*, at 199. It would indeed be a "bootless task, involving judgments remote from the experience and competence of the judiciary" for the Board to undertake to determine an individual's fitness for assignment to a particular kind of classified work or his or her trustworthiness for access to classified information or areas. *Greene v. McElroy*, *supra*, at 953. The delicate question of whether to issue or revoke a clearance for access to classified information, depending as it does on the "compass" of accumulated agency expertise to guide an adjudicator to the proper resolution of many factors on an individual basis,[13] is as discretionary and as demanding a determination as virtually any of the Executive decisions in which the federal judiciary has previously refused to intervene. *E.g.*, *Tennessee v. Dunlap*, 426 U.S. 312, 315-16 (1976)(state National Guard decision not to permit plaintiff to reenlist was not reviewable, notwithstanding the fact that the state's decision caused plaintiff to be removed from federal civil service under conditions that might otherwise have been reviewable); *Gilligan v. Morgan*, *supra*, at 10-11, 12 (training, equipping, and operating the Armed

---

[12] Even in more routine agency matters, courts will not review agency actions that are "committed to agency discretion by law." 5 U.S.C. §701(a)(2); *Hondros v. United States Civil Service Commission*, 720 F.2d 278, 292 (3d Cir. 1983). In personnel security clearance cases, this "law" is the Constitution and the Congressional policy that is intended to govern this area. *See* parts I.C.2.,3., *supra*.

[13] The Department of Defense, for example, handled over 796,000 security clearance applications in fiscal year 1983 alone.

Forces); *Orloff v. Willoughby*, *supra*, at 90, 92, 93-95 (military appointments and duty assignments); *NeSmith v. Fulton*, 615 F.2d 196, 203 (5th Cir. 1980)(dismissal of a member of the Air National Guard, resulting in his removal from federal civilian employment); *West v. Brown*, 558 F.2d 757, 760-61 (5th Cir. 1977), *cert*. *den*., 435 U.S. 926 (1978)(Army regulation barring the enlistment of unwed parents of minor children); *American Federation of Government Employees v. Hoffman*, 427 F.Supp. 1048, 1053, 1081-82 (N.D.Ala. 1976)(determination of the appropriate civil servant-contractor personnel mix in the performance of a defense contract for the production of ballistic missiles); *Turner v. Egan*, 358 F.Supp. 560, 564 (D.Alas.), *aff'd*, 414 U.S. 1105 (1973) (determination of what officers are sufficiently qualified for retention in the Armed Forces). Even the Board itself has refused to review a decision involving specialized agency judgment. *Schaffer v. Department of the Air Force*, 6 MSPB 631, 633-34 (1981)(declining to review, where the challenged decision was made in accordance with the agency's own regulations and had no constitutional ramifications, whether the Air Force Reserves were justified in treating the plaintiff differently than other overweight reservists). Agency security clearance determinations are a fundamental - indeed, critical - part of the national defense: the rigorous process of training, equipping, and assigning members of the Armed Forces throughout the world will ultimately be of little value to the Nation if classified information itself cannot be protected. Surely the Executive's expert judgments on access to classified information are due at least the same deference as its decisions concerning overweight airmen.

c. Prudential considerations.

Finally, prudential considerations also counsel against the Board's intervening to review or challenge the factual bases of Executive Agencies' security clearance determinations.

In each of the cases sub judice - and in all cases involving Executive Agencies' personnel security clearance determinations - the agencies concerned have made an informed, expert decision on whether an individual's eligibility for or access to classified information is clearly consistent with the interests of national security. The Board's intervening to review the factual bases for and the wisdom of these determinations upsets the delicate balance that has been developed by the Executive and Congress and forces the Board to render unintended policy assessments on such issues as who shall have access to classified information, when, and under what conditions. If the Board itself gives certain individuals eligibility for - or worse, actual access to - classified information, the Executive must restructure its entire personnel security program to become a re-active one, not an active one, one which does not protect the national security but rather attempts to minimize the potential damage. The existing personnel security program is intended to permit an agency to make a final determination at the outset and, thereafter, carry out the business of protecting the national security. The Board's review will create uncertainty in the agencies (as well as among their employees) regarding an individual's security status; make peers, supervisors, and subordinates unable to rely on the current presumption that those cleared for access to classified information are unquestionably trustworthy and able to protect such information; and overburden limited agency manpower resources by necessitating constant management of and compensation for those who, because of the Board's orders, are in a position to do irreparable harm to the national security. In an area as critically important as that involving the protection of classified information, our nation must speak with a single, clear voice - unhampered by the imprecise second-guessing of those who are neither trained nor sufficiently prepared to do so. See part II, infra (only the Executive is in a position to be accountable for the ultimate results of security clearance determinations).

d. Summary.

In summary, the Board should, and must, defer to Executive Agencies' security clearance determinations when, as here, the agencies acted in accordance with their own regulations; no constitutional issues are raised; the area is one committed to the Executive (as security clearance determinations are); and the agencies possess superior expertise on, knowledge of, and experience in the subject matter concerned. The Board's continuing to force Executive Agencies to reinstate security clearances - or even its continuing to review the merits of agencies' security clearance determinations at all - actually undermines the Executive by inviting confusion into an area that leaves no room for mistakes or second chances. Fundamental constitutional and political considerations dictate otherwise:

> In a mature democracy, choices such as [those involving classified defense information] must be made by the executive branch, and not by the judicial. If too many mistakes are made, the electorate will in due time reflect its dissatisfaction with the results achieved. It would be an unwarranted interference with the responsibility which the executive alone should bear, were the judiciary to undertake to determine for itself whether . . . any . . . individual . . . is in fact sufficiently trustworthy to be entitled to [a] security clearance . . .

Greene v. McElroy, 254 F.2d 944, 954 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959).

II. IN ANY EVENT, THE BOARD CANNOT ORDER AN EXECUTIVE AGENCY TO ISSUE OR REINSTATE A PERSONNEL SECURITY CLEARANCE OR GRANT TO AN INDIVIDUAL ACCESS TO CLASSIFIED INFORMATION OR CONTROLLED AREAS.

As discussed hereinbefore, the Board - for legal, prudential, and practical reasons - lacks the authority to review the merits of Executive Agencies' security clearance determinations, including those made in the cases at bar. If, however, the Board does choose to review the merits of the agencies' security clearance determinations in these cases and disagrees with the conclusions originally reached, it may only direct the agencies to re-exercise their discretion and, if necessary, reconsider their earlier security decisions.

First, the Board has recognized that it cannot order agencies to take actions that are not appealable to the Board. Barger v. Department of Justice, 10 MSPB 148, 152 (1982). Like matters involving agency expertise on issues of judgment and choice that are left to the agency's informed discretion, and thus not subject to judicial writs of mandamus, see, e.g., California v. Settle, 708 F.2d 1380 (9th Cir. 1983), the actual issuing of personnel security clearances and the granting of access to classified information and areas is an Executive action that is not appealable to the Board. See part I.C.1., supra.

Secondly, an important key to the legitimacy of the existing process of determining whether an individual's eligibility for or access to classified information is clearly consistent with the interests of national security is the Executive accountability that this determination carries with it:

> [T]here is a reasonable basis for the view that an agency head who must bear the responsibility for the protection of classified information committed to his custody should have the final say in deciding whether to repose his trust in an employee who has access to such information.

Cole v. Young, 351 U.S. 536, 546 (1956). Accord, Greene v. McElroy, 254 F.2d 944, 954 (D.C. Cir. 1958), rev'd on other grounds, 360 U.S. 474 (1959)(in a mature democracy, the Executive is accountable to the electorate on matters such as the handling of classified information). If an Executive Agency incorrectly grants access and a compromise occurs, or if a clearance is denied for improper reasons, an existing system of checks and balances will come into play - depending upon the situation, the Executive must answer to Congress, the federal courts, and the electorate. If, however, the Board errs and a compromise of defense secrets occurs, there will be no one to whom the Nation can turn for the difficult answers or the necessary assurances that subsequent measures will prevent similar occurrences.

Being unable to order an agency to take an action (such as a personnel security determination) that is not itself appealable to the Board and being ill-suited to make highly specialized and far-reaching security clearance decisions or to account for the ultimate effects of its orders in an area leaving no room for second chances, the Board must refrain from usurping the Executive's delicately balanced function of protecting the security of our Nation. See Haig v. Agee, 453 U.S. 280, 307 (1981)("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.").

CONCLUSION

For the foregoing reasons, the Board must decline to review the merits of the Executive Agencies' expert determinations to revoke the personnel security clearances in the cases at bar.

Respectfully submitted,

L Niederlehner

LEONARD NIEDERLEHNER
Acting General Counsel
Department of Defense

Kathleen A. Buck

KATHLEEN A. BUCK
Assistant General Counsel for
Legal Counsel
Department of Defense

John R. Mo

JOHN R. MORRIS
Attorney-Advisor
Office of Legal Counsel
Department of Defense

Pentagon, Room 3E980
Washington, D.C. 20301-1600

Telephone: (202) 695-3341

QUESTIONS SUBMITTED FOR WRITTEN RESPONSE

HEARINGS BEFORE THE
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
ON
FEDERAL GOVERNMENT SECURITY CLEARANCE PROGRAMS

APRIL 1985

* * * *

KATHLEEN A. BUCK
Assistant General Counsel
DEPARTMENT OF DEFENSE

QUESTION: Can you tell us briefly the facts of the Hoska case?

RESPONSE: Lukas E. Hoska, prior to his dismissal from employment, was an Intelligence Operations Specialist with the U.S. Army Administration Survey Detachment. In October 1979, approximately four years after being hired, and while stationed in West Berlin, Mr. Hoska's Top Secret security clearance was revoked. The revocation was based on allegations of security violations by him, an unfavorable psychiatric evaluation, and several incidents of allegedly indiscreet behavior which, the Army concluded, reflected poor judgment and emotional instability. Because he no longer had a security clearance which was necessary for him to perform his duties Mr. Hoska was dismissed.

QUESTION: What is your view of the long term implications of the Hoska decision?

RESPONSE: If the Hoska case remains intact and is relied upon by other courts as a precedent, I believe the courts and the Merit Systems Protection Board (MSPB) will be second guessing agencies on the issue of whether an individual applicant for a security clearance is trustworthy. I foresee the courts not only substituting their judgment for agency decisions to revoke or deny a clearance, but also sustituting their personal opinions for agency decisions on what positions require security clearances. The delicate Executive function of protecting our national security by ensuring the trustworthiness of employees who work with classified information or in classified areas is slowly being usurped by the judiciary and the MSPB.

QUESTION: Has the Merit Systems Protection Board initiated any action because of the Hoska decision?

RESPONSE: The Board has at least recognized that the Board's involvement in security clearance cases raises serious jurisdictional questions following the Hoska decision. The Board has requested and received amicus briefs on this issue.

QUESTION: Could the Army have established a "nexus" for its action in the Hoska case? If so, why did it not do so?

RESPONSE: In Hoska the court actually ordered the clearance reinstated rather than remand the case for a hearing consistent with the court's opinion. The record before the MSPB was developed by the Army based on historical precedent and practice. The Hoska decision appears to shift the burden of establishing trustworthiness from the applicant for the clearance to the Government. In litigating security clearance cases following the Hoska decision the Army has tenaciously attempted to establish a "nexus" in each case.

QUESTION: If you do believe that Hoska represents a turning in judicial intervention in the personnel security system, is it the Defense Department's position that this is an unwise development?

RESPONSE: I believe that Hoska is an erroneous decision. The *amicus* brief filed by the Department of Defense with the MSPB discusses this issue at length. Who should be entrusted with the secrets of our country is a very difficult national security decision. Within the Department we have experts who deal with this issue on a daily basis and we believe it is reasonable for the courts to accord great deference to our national security experts.

QUESTION: Does the Pentagon have a policy with regard to homosexuals who are candidates for, or who hold, security clearances?

RESPONSE: Decisions in all security clearance cases are on a case-by-case basis, depending upon the particular facts and circumstances in each case. Among the factors to be considered is whether a particular individual has engaged in or engages in acts which are criminal, reckless, or irresponsible; constitute sexual perversion; indicate lack of judgment or instability; or may subject the individual to coercion or pressure causing action contrary to the national interest. In cases which involve sexual perversion, it is also relevant whether the particular conduct is criminal in the jurisdiction in which the subject resides; whether the conduct occurs in public or private; whether it is consensual; whether it involves minors; whether it is indicative of instability or bad judgment; and whether in the given case the individual is vulnerable to blackmail or otherwise may be coerced so as to act contrary to the national interest. All these factors, when considered together or individually, may support a conclusion in a particular case that the granting or continuation of a security clearance is not clearly consistent with the national security.

The ultimate determination as to whether a person meets the standard must be an overall commonsense determination based on all available information. Consideration is also given to such factors as the seriousness of the facts and circumstances; the recency and motivation for the conduct in question; the extent to which it was voluntary and undertaken with specific knowledge of the circumstances involved, and, to the extent to which it can be estimated, the probability that such conduct will continue. I stress that it is DoD policy to evaluate each case on its facts and there is no per se rule with respect to homosexuals.

QUESTION: Can you provide the Subcommittee with the distinction between a suitability clearance and a security clearance?

RESPONSE: We do not have a "suitability" clearance. The terms "suitability" and "eligibility for access to classified information" are often confused. A person is evaluated for access to classified information based on the criterion of "clearly consistent with the national security." An unfavorable determination simply means that no security clearance will be issued. "Suitability" on the other hand, is evaluated in terms of one's ability to perform his or her specific job. For example, a convicted espionage agent may be an excellent typist who could perform a typist's job very well but be considered untrustworthy to handle classified information.

QUESTION: Does the Pentagon have to look at both suitability clearances and security clearances in the adjudication process? If so, why?

RESPONSE: The Defense Department adjudicates only security clearances. While information concerning an employee may have both suitability and security significance, separate judgments will be made.

QUESTION: As seen in the Hoska case and other recent cases, is there a tendency in the courts to judge applicants for security clearances only in terms of suitability and not security?

RESPONSE: Yes, we have seen opinions issued at the Merit Systems Protection Board and by courts which appear to declare that a person deserves access to classified information because the person is a hard worker regardless of other adverse information in the record. It is important to recognize that our security program is based on preventive action and weighing of the risks.

QUESTION: How would you rectify this tendency to blend the suitability and security issues?

RESPONSE: The President currently has a task force working on a complete revision of Executive Order 10450 which addresses the issue of security for the Executive branch. We expect the task force to specifically examine this problem.

QUESTION: Has the Socialist Workers Party been a subject of special interest to personnel security officials in the Defense Department? If so, why?

RESPONSE: The Department is currently in litigation with the Socialist Workers Party and, therefore, it would be inappropriate to comment. The longstanding position of the Department has been, however, that security clearance decisions cannot be based on ignorance and our investigators should be able to ask questions concerning criminal conduct and the disposition of classified information.

QUESTION: In pre-hearing interviews with the Subcommittee staff, you mentioned the uncertainties in personnel security programs caused by efforts to rehabilitate alcoholics and drug addicts. Is it apparent that certain of these rehabilitation programs may require the Defense Department to keep some persons on the job because they are undergoing rehabilitation when in fact they are still abusing alcohol or drugs and, as such, may themselves be security risks?

RESPONSE: When passing the law on rehabilitation programs (See 42 U.S.C. 290dd-1(c), 290ee-1(c)) I believe that Congress never intended to permit individuals with drug and alcohol problems to argue they are entitled to a security clearance because they are "handicapped." Unfortunately, this issue is being raised by some applicants for security clearances and we are concerned that a court could accept this argument.

QUESTION: The due process procedures applied in the industrial security program have generally not been subject to attack by the courts. Could you explain why?

RESPONSE: The due process procedures which are followed in the industrial security program are very detailed and are comparable to a mini-trial. In fact, we are examining ways in which we could streamline the procedures to make decisions on a more timely basis.

QUESTION: The due process guarantees have been significant to civilian courts when they rule on suitability and clearance cases from the armed services? Will you give your view as to why?

RESPONSE: The due process analysis has been applied to all security clearance cases. The courts have been careful to ensure that procedural safeguards have been followed before clearances are revoked or denied. The reasoning is based on the Supreme Court case of Greene v. McElroy, 360 U.S. 474 (1959) which held that in the absence of explicit authorization from either the President or the Congress the Department was not authorized to deprive a person of his job in a proceeding in which he was not afforded the safeguards of confrontation and cross-examination.

Senator NUNN. We have numerous statements that will be admitted for the record.

We also have my closing statement which I will insert, without objection, although we have gone over a great deal of the points I made in that closing statement, and we will keep the record open for 2 weeks.

[Senator Nunn's closing statement follows:]

CLOSING STATEMENT OF SENATOR SAM NUNN

As we conclude these 4 days of hearings, I would like to make a few closing remarks.

First, I want to express my gratitude to Chairman Roth and his Majority staff for the support and cooperation they have given in the hearing room and over these many months in preparation for the hearings.

Second, I want to thank Senator Gore, who has just become a member of the subcommittee, for participating in, and contributing to, the hearings.

Looking back upon the testimony, it becomes readily apparent that the government's personnel security programs are in need of review and reform.

In the next few weeks, members and staff are going to examine several issues for possible inclusion in the subcommittee's final report with findings, conclusions and recommendations for corrective action.

Among the issues the subcommittee will consider addressing will be the possible need for legislation to strengthen or replace Executive Order 10450, the basic authority upon which Government's personnel security programs are based. E.O. 10450 is three decades old and several witnesses expressed the opinion that a fresh approach is needed. One problem which such legislation could address would be the need for some degree of uniformity and consistency in the way various Government agencies investigate and adjudicate requests for security clearance.

A second principal issue the subcommittee may address has to do with devising an effective way to control—and preferably reduce—the number of requests for clearances. Incentives may be needed to encourage managers in Government, as well as in the defense industrial sector, to ask for clearances only for those workers and executives who truly require them to carry out their assignments. Hearing testimony seriously questioned whether all of the 4.2 million Americans who today hold clearances have or even need access to classified materials. The investigative process has become too costly to justify the granting of clearances on the basis of convenience or status.

Similarly, once a person has received a clearance, Government should make every effort to periodically monitor that person from a security point of view as his life circumstances change. Hearing testimony emphasized the fact that the Government's reinvestigation procedures are today woefully inadequate. Unfortunately, reinvestigations are expensive. That is all the more reason to keep control over the numbers of clearance recipients.

Testimony underscored again and again the obvious lack of sufficient Government investigative manpower in the face of an increasingly large workload, particularly in the industrial sector. The subcommittee may wish to consider ways in which industry can assume a more active role in the personnel security program—as in periodically recertifying the need for clearances or in regularly updating personnel security information.

Several witnesses cited the importance of setting uniform standards for the training of personnel security investigators and adjudicators. That too is an issue the subcommittee may wish to address in its recommendations for corrective action.

Regarding plant security, we have seen in the testimony of Mr. Boyce how easily classified information can be compromised when proper controls are not applied, and rigorously enforced, on one who enjoys passage to and from sensitive areas. The subcommittee may wish to consider the need to strengthen incentives for contractors to maintain and continually upgrade plant security measures and increase penalties when they do not.

We have seen the difficulties in verifying information abroad that arise when immigrant aliens and recently naturalized citizens apply for security clearances. It is hoped that more effective ways to investigate these applicants can be developed so that their talents can be fully utilized in national security areas.

Finally, the subcommittee may consider urging the executive branch to initiate a Government-wide evaluation of personnel security programs, with an eye toward a major overhaul. Progress can be achieved, but all the principal players in the process—the Pentagon, the Office of Personnel Management, the Justice Department, the National Security Council and others—must work in harmony. The issue is too important for success to be blocked by bureaucratic turf battles, indecision and delay.

Senator NUNN. I want to thank Mr. Rinzel and the majority staff for your splendid assistance and cooperation in these hearings. I want to thank Eleanore Hill and the minority staff for a very thorough investigation, and I want to, after patting staff on the back, say that while the memory of this hearing is still hot, I would like to have an extensive number of options for consideration of the Senators in terms of what we would recommend. I think we want to press forward on this, and I would envision that once we come up with a list of recommendations that we will get together in an informal way with key players in the executive branch, including key players who recently retired and try to bounce away some of these ideas. We may not reach unanimous agreement, but I think that will be the best way to proceed.

We will at some point, we hope in the near future, issue a set of recommendations. Of course, this subcommittee is investigative in nature, and not legislative. A number of us will be introducing, I am sure, some changes in law. We thank you all for being here, thank the staff for a splendid job and the hearings will be recessed.

[Whereupon, at 11:30 a.m., the subcommittee adjourned to reconvene at the call of the Chair.]

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

DOE 5631.2A

D R A F T
9-11-84
[illegible]

PERSONNEL SECURITY PROGRAM

1. PURPOSE. To establish the policy, responsibilities, and authorities for implementing the Department of Energy (DOE) personnel security program.

2. CANCELLATION. DOE 5631.2, PERSONNEL SECURITY PROGRAM, of 11-13-80.

3. SCOPE. The provisions of this Order apply to all Departmental Elements. The personnel security program of the Department of Energy applies to its employees and contractors, as follows:

   a. The provisions of the Atomic Energy Act of 1954, as amended, Executive Orders 10450 and 12356, and Federal Personnel Manual Chapter 732 apply to Departmental employees, applicants for employment, consultants, employees of other Federal agencies, and assignees for employment and access.

   b. The provisions of the Atomic Energy Act of 1954, as amended, Executive Orders 10865 and 12356 apply to Departmental contractors, subcontractor employees and consultants, and access permittees for access.

4. POLICY AND OBJECTIVES.

   a. It is DOE policy to afford DOE employment, and/or access to Restricted Data, National Security Information and other sensitive data, and/or category I or category II quantities of special nuclear material to individuals whom the DOE has made a determination that such employment and/or access will not endanger the common defense and security and is clearly consistent with the national interest. Except as authorized by the Secretary (or designee) that such action is clearly consistent with the national interest, this determination shall be based upon an investigation and report by the Office of Personnel Management or the Federal Bureau of Investigation. The determination may also be based upon investigation conducted by another Government agency which conducts personnel security investigations, provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individuals by another Government agency based on such an investigation and report.

   b. Requests for clearances shall be submitted only after a determination has been made that the duties of a position require access to classified information, or special nuclear material in category I or II quantities,

All Departmental Elements

Office of Safeguards
and Security

or regular access to a security area. Clearances are not to be requested as a means for alleviating individual or management responsibility to safeguard classified information on a "need-to-know" basis nor is one to be used as a means to determine suitability for Government employment. It is the intent of this policy to assure that clearances are requested only when absolutely required, to avoid the unnecessary expenditure of agency funds and resources or the unwarranted invasion of an individual's right to privacy.

(1) The DOE will take all reasonable measures to obtain existing reports of investigation which may fulfill the agency standards and specifications as to the scope and extent of investigations established by the Secretary.

(2) Requests for clearances will not be processed: (a) unless all required security forms are completed and signed (when appropriate) by the applicant; (b) if the printed content of the security forms has been altered; or (c) if insufficient information is provided or the forms are illegible.

(3) The possession of a DOE clearance permits an individual access to the levels of classified information (on a "need-to-know" basis) as shown in Attachment 1.

5. REFERENCES.

a. Atomic Energy Act of 1954, as amended, Section 143, "Department of Defense Participation;" Section 145, "Restrictions;" and Section 161.b, "General Provisions," which are the legislative requirements for establishment of a DOE security program for controlling access to Restricted Data and special nuclear material.

b. 10 CFR Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material," which is used in those cases in which there are questions of eligibility for DOE access.

c. DOE 1360.2, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS, of 3-9-79, which establishes policies and procedures for developing, implementing, and administering a program for safeguarding DOE computer systems and, in particular, DOE sensitive unclassified information.

d. Executive Order 10450, "Security Requirements for Government Employees," of 4-27-53, as amended, which establishes the requirement for determining that all Federal employees be loyal, reliable, trustworthy, and of good conduct and character.

e. Executive Order 10865, "Safeguarding Classified Information Within Industry," of 2-24-60, as amended, which establishes the basis for the industrial security program for civilian personnel.

f. Executive Order 12356, "National Security Information," of 4-2-82, which establishes controls on access to classified information.

g. Federal Personnel Manual, Chapter 731, "Personnel Suitability," which contains requirements determining position sensitivity and requirements for for employment by the Government regarding the character, reputation, and fitness of the individual under consideration.

h. Federal Personnel Manual, Chapter 732, "Personnel Security," which implements Executive Order 10450 throughout Federal departments and agencies.

i. Federal Personnel Manual, Chapter 736, "Personnel Investigations," which deals primarily with National Agency Checks and Inquiries (NACI), and full field investigations conducted by the Office of Personnel Management.

j. Federal Personnel Manual Letter 732-7, "Personnel Security Program for Position Associated with Federal Computer Systems," which establishes policy for a personnel security program covering positions that are involved in the design, storage, retrieval, access, and dissemination of information maintained in Federal computer systems, as well as positions associated with automated decisionmaking systems.

k. Office of Management and Budget Circular No. A-71, "Security of Federal Automated Information Systems," of 7-27-78, with Transmittal No. 1, which promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch Departments and Agencies.

6. DEFINITIONS.

a. Access.

(1) The knowledge, use, or possession of classified information or other sensitive information which is required by an individual in the performance of official duties and which is provided to the individual on a "need-to-know" basis.

(2) Or situations involving the responsibilities of an individual in the performance of official duties which may provide proximity to or control over special nuclear material in category I or II quantities.

b. Access Authorization or Security Clearance. An administrative determination that an individual who is either a DOE employee, applicant for employment, consultant, assignee, other Federal department or agency employee (and other persons who may be designated by the Secretary of Energy), or a DOE contractor or subcontractor employee, is eligible for access to Restricted Data, other classified information, or special nuclear material. Clearances granted by the DOE are designated as "Q," "L," "Top Secret," or "Secret."

(1) "Q" Access Authorizations or Clearances are based upon full field investigations conducted by the Federal Bureau of Investigation, Office of Personnel Management, or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need-to-know" basis, to Top Secret, Secret and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in category I or II quantities as required in the performance of duties. When "Q" access authorizations or clearances are granted to employees of access permit holders they are identified as "Q(X)" access authorizations or clearances and permit access only to the type of Secret Restricted Data specified in the permit.

(2) Top Secret Access Authorizations or Clearances are based upon full field investigations conducted by the Office of Personnel Management or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need-to-know" basis, to Top Secret, Secret, and Confidential National Security Information and Formerly Restricted Data as required in the performance of duties.

(3) "L" Access Authorizations or Clearances are based upon National Agency Check and Inquiries (NACI) for Federal employees, or National Agency Check with Credit (NACC) for non-Federal employees, conducted by the Office of Personnel Management. They permit an individual access, on a "need-to-know" basis--to Confidential Restricted Data; to Secret and Confidential Formerly Restricted Data; and to Secret and Confidential National Security Information required in the performance of duties, provided such information is not designated "CRYPTO" (classified cryptographic information), other classified communications security ("COMSEC") information, or intelligence information. When "L" access authorizations or clearances are granted to employees of permit holders, they are identified as "L(X)" access authorizations or clearances and permit access only to the type of Confidential Restricted Data specified in the access permit. Additionally, the cognizant DOE official may grant an "L" access authorization or clearance to craft or manual workers, community management and service personnel, nurses, medical technicians, cafeteria workers, health and safety workers, purchasing and accounting groups, and the like, who are employed in classified construction or operations areas, provided the work of such individuals does not afford them:

(a) More than visual access to buildings and equipment classified not higher than Secret Restricted Data.

(b) Or access to information classified higher than Confidential Restricted Data concerning plant operating characteristics, process data, weapons, or weapons components.

(4) Secret Access Authorizations or Clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks with Credit (NACC) for non-Federal employees, conducted by the Office of Personnel Management. They permit an individual access on a "need-to-know" basis, to Secret and Confidential National Security Information as required in the performance of duties.

c. Access Permittee. An individual or organization which has been issued a permit by the Department of Energy, providing access to Restricted Data applicable to civil uses of atomic energy in accordance with the terms and conditions stated on the permit and in accordance with applicable security regulations.

d. Classified Information. Any information which requires protection against unauthorized disclosure in the interests of the national defense and security or foreign relations of the United States pursuant to U.S. statute or Executive order. The term includes Restricted Data, Formerly Restricted Data, and National Security Information, each of which has degrees of importance denoted by the classifications Top Secret, Secret, or Confidential.

e. Derogatory Information. Unfavorable information concerning an individual which creates a question as to the individual's eligibility or continued eligibility for access or employment.

f. Formerly Restricted Data. Classified information jointly determined by the Department of Energy (or its predecessors, the Atomic Energy Commission and the Energy Research and Development Administration) and the Department of Defense to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

g. Hearing Counsel. A DOE attorney assigned to prepare and present a Personnel Security Hearing before a Hearing Officer.

h. Hearing Officer. An individual appointed by the manager of the operations office who, upon considering the evidence at a hearing, makes specific findings as to the truth of the derogatory information, and determines whether to recommend to the manager of the operations office the granting, denial, or revocation of an individual's access authorization. Hearing Officers shall be U.S. citizens and have a DOE "Q" clearance.

i. Interim Access Authorization. A determination by the Secretary, for access to National Security Information, or by the Assistant Secretary for Defense Programs, for access to Restricted Data, that it is clearly consistent with the national interest for the DOE to permit an individual to have such access prior to the DOE's receipt of full field reports of investigation. Interim access authorizations are not processed for access permittees or for those individuals whose accesses will require an "L" or Secret clearance.

j. Managers of Operations Offices. The managers of the DOE operations offices, the Manager of Pittsburgh Naval Reactors Office, the Manager of Schenectady Naval Reactors Office, and at Headquarters, the Director of Safeguards and Security, (DP-34).

k. National Security Information. Information which requires protection in the interest of national defense or foreign relations of the United States and classified in accordance with an Executive order which does not fall within the definition of Restricted Data or Formerly Restricted Data.

l. Naval Nuclear Propulsion Information. All information classified or unclassified concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships, including the associated nuclear support facilities.

m. Need-to-Know is an official determination, by a division director or higher official, that an employee, contractor, or properly cleared individual requires access to the specific classified information in the performance of official duties.

n. Personnel Security Review Examiners. Persons appointed by the DOE Assistant Secretary for Defense Programs who are designated to review questions concerning the eligibility or continued eligibility of those individuals described in 10 CFR Part 710.2. Examiners shall be U.S. citizens and have a DOE "Q" clearance.

o. Position Sensitivity Designation. A written certification by the appropriate DOE official that a position under his or her jurisdiction (to be occupied by a DOE employee, applicant for employment, consultant, or assignee) is Special-Sensitive, Critical-Sensitive, Noncritical-Sensitive, or Non-Sensitive.

p. Restricted Data. Data which is defined in section 11y of the Atomic Energy Act of 1954, as amended, as "...all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142."

q. Security Area. A physically defined space containing classified matter (documents or material) or special nuclear materials subject to physical protection and personnel access controls.

r. Sensitive Data. Information requiring a degree of protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data, sensitive energy data, sensitive financial or supply data).

s. Special Nuclear Material. Special nuclear material, as defined in Section 11 of the Atomic Energy Act of 1954, as amended, not subject to a Nuclear Regulatory Commission license. For the purpose of this Order, special nuclear material in one facility or shipment is divided into the following categories:

(1) Category "I" Quantities of Special Nuclear Material.

(a) Uranium 235 (contained in uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with plutonium and uranium 233 when (multiplying the plutonium and/or uranium 233 content by 2.5) the total is 5,000 grams or more.

(b) Plutonium and/or uranium 233 when the plutonium and/or uranium 233 content is 2,000 grams or more.

(c) Special nuclear material in lesser quantities but which is located in the same area of shipment with other special nuclear material with which it could be selectively combined to produce the equivalent quantities in subparagraphs (1) or (2) of this category.

(2) Category "II" Quantities of Special Nuclear Material.

(a) Uranium 235 (contained in uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with plutonium and uranium 233 (multiplying the plutonium and/or uranium 233 content by 2.5) when the total is 1,000 to 4,999 grams.

(b) Plutonium and/or uranium 233 when the plutonium and/or uranium 233 content is 400 grams to 1,999 grams.

(c) Special nuclear material in lesser quantities but which is located in the same area or shipment with other special nuclear material with which it could be selectively combined to produce the equivalent quantities in subparagraphs (1) or (2) of this category.

7. RESPONSIBILITIES AND AUTHORITIES.

a. The Secretary of Energy.

(1) Certifies those specific positions which are of a high degree of importance or sensitivity under Section 145f of the Atomic Energy Act of 1954, as amended, which are to be the subject of an investigation by the Federal Bureau of Investigation.

(2) Designates those specific positions within DOE which are sensitive under Section 3(b) of Executive Order 10450.

(3) Authorizes, in the case of emergency, and for a limited period of time, a Critical-Sensitive position to be occupied within the DOE by an individual for whom a preappointment full field investigation has not been completed, if such action is an emergency and necessary in the national interest under Section 3(b) of Executive Order 10450.

(4) Grants authorization for access to National Security Information pursuant to Section 4.1(a) of Executive Order 12356 prior to completion of the required investigation when it has been determined that such action is in the national interest.

(5) Establishes standards and specifications in writing as to the scope and extent of investigations under Section 145g of the Atomic Energy Act of 1954, as amended.

(6) Makes determinations required by 10 CFR Part 710.27(m)(2) and 10 CFR Part 710.33.

b. The Assistant Secretary for Defense Programs (DP-1).

(1) Grants authorization for access to Restricted Data pursuant to section 145b of the Atomic Energy Act of 1954, as amended, prior to completion of the required investigation when he has determined that such action is in the national interest.

(2) Issues subpoenas to witnesses in all cases processed in accordance with 10 CFR Part 710.20 et seq.

(3) Acts as "special designee" under 10 CFR Part 710.27(m)(2) to determine whether statements may be received by a Hearing Officer and determine whether new evidence may be received in accordance with 10 CFR Part 710.29(b)(2).

(4) Submits records in administrative review proceedings in accordance with 10 CFR Part 710.30(d)(2) and (e).

(5) Grants, denies, or revokes access authorization in accordance with 10 CFR Part 710.24(a) and 710.32.

(6) Approves reconsideration of access authorization cases in accordance with 10 CFR Part 710.34.

(7) Designates the individuals who offer findings and recommendations in administrative review cases in accordance with 10 CFR Part 710.31.

c. Heads of Departmental Elements.

(1) Generates requests to the Secretary for waivers of preappointment full field investigation requirement for candidates under consideration to occupy Critical-Sensitive positions.

(2) Generates requests to the Secretary or the Assistant Secretary for Defense Programs (DP-1), through the Director of Safeguards and Security (DP-34), for interim access authorizations.

d. General Counsel.

(1) Approves, and in those cases where authorized by the manager of operations office, prepares notification letters to individuals whose eligibility for access authorization is in question in accordance with 10 CFR Part 710.22.

(2) Concurs in request for suspensions in cases processed in accordance with 10 CFR Part 710.21.

e. Heads of Headquarters Elements.

(1) Certify in writing to the Director of Personnel (MA-20), position sensitivity designations for each position under their jurisdiction to be occupied by a DOE employee or applicant for employment, consultant, or assignee.

(2) Approve and transmit to the Director of Safeguards and Security (DP-34) requests for access authorization of employees of other Federal departments or agencies who require access to Restricted Data.

(3) Approve for consideration, and transmit to DP-34, applications for access authorizations for foreign nationals.

(4) When required, furnish "Data Report on Spouse" (DOE Form DP-354) for personnel under their jurisdiction who possess an access authorization.

(5) Approve and transmit to DP-34 requests for access authorizations for members of the Armed Forces and civilian employees of the Department of Defense and the National Aeronautics and Space Administration assigned to duty with DOE Headquarters organizations, for access to Restricted Data.

f. Director of Personnel (MA-20).

(1) Receives, reviews, and concurs in the certifications of position sensitivity designations, and, if applicable, associated security clearance requirements for Headquarters positions to assure compliance with the guidelines contained in Chapter I.

(2) Provides copies of certifications of position sensitivity designations to DP-34.

(3) Processes all requests for investigations for DOE Headquarters employees, applicants for employment, consultants, and assignees to DP-34.

(4) Determines final action to be taken in those cases where questionable suitability information is developed.

(5) When required, makes a determination to continue processing requests for waivers of preappointment full field investigations.

g. Director of Safeguards and Security (DP-34).

(1) Develops policy, objectives, standards, guides, and procedures for the DOE personnel security program.

(2) Authorizes managers of operations offices to initiate security investigations relative to foreign nationals who are applicants for security clearance.

(3) Performs the functions assigned to the Director, Safeguards and Security, and make recommendations to the Assistant Secretary for Defense Programs as appropriate for cases processed in accordance with the provisions of 10 CFR Part 710.20 et seq. and 10 CFR Part 710.38.

(4) Processes all requests by other Government agencies for verification of an individual's DOE security clearance status.

(5) Maintains centralized records for all DOE security clearance actions.

(6) Coordinates requests by the Inspector General for access to personnel security information for investigative purposes.

(7) Approves and maintains records of review of Headquarters personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.

(8) Recommends to the Controller funding necessary for conducting personnel security investigations.

(9) Maintains liaison with the Federal Bureau of Investigation and the Office of Personnel Management and is principal point-of-contact with these agencies on all personnel security matters.

(10) Notifies the Federal Bureau of Investigation or Office of Personnel Management of withdrawals of requests for investigation.

(11) Initiates:

(a) Investigation of spouses of individuals who marry after having been processed for an access authorization.

(b) Appropriate investigation and grants access authorizations for access to Restricted Data for:

(1) Personnel of the Department of Defense and the National Aeronautics and Space Administration assigned for duty with DOE or DOE contractors or with other Federal Departments or Agencies.

(2) Employees of other Federal Departments or Agencies who require such access.

(12) Accepts properly executed certifications for Department of Defense and National Aeronautics and Space Administration personnel assigned for duty with DOE who require access to Restricted Data.

(13) Concurs in requests to the Secretary for waivers of preappointment full field investigation requirements for candidates under consideration to occupy Critical-Sensitive positions.

(14) Accepts properly executed requests for interim access authorizations, conducts appropriate indices checks (such as name checks with other Government agencies), and forwards such requests to the Assistant Secretary for Defense Programs (DP-1) with appropriate recommendations.

(15) Performs the following functions for DOE Headquarters, energy technology centers, and power marketing agencies:

(a) Implements the personnel security program consistent with the policy, standards, guides, and procedures stated in this Order and in 10 CFR Part 710.

(b) Performs functions listed on pages 12 and 13, paragraphs 7h(2) through 7h(8), and 7h(12).

(c) Performs functions listed on page 14, paragraphs 7h(15)(a) through 7h(15)(e) and 7h(15)(g) through 7h(15)(l).

(d) Makes an annual compilation of "positions of a high degree of importance or sensitivity" for certification.

(e) Processes "Data Reports on Spouse" (DOE Form DP-354).

(f) Processes cases of DOE or DOE contractor personnel who are hospitalized or otherwise treated for a mental illness which may cause a defect in judgment or reliability.

(g) Evaluates all reports of investigation conducted on DOE employees and applicants for employment for suitability in sensitive positions, and notifies the Director of Personnel of the results of each investigation for appropriate action.

h. Managers of Operations Offices.

(1) Implement the personnel security program consistent with the policy, standards, guides, and procedures stated in this Order and in 10 CFR Part 710.

(2) Authorize suspension of access authorization in accordance with 10 CFR Part 710.21.

(3) Initiate requests for investigation directly to the Federal Bureau of Investigation or Office of Personnel Management.

(4) Determine the position sensitivity and access requirements prior to requesting investigations for DOE employees or applicants for employment, consultants, and assignees.

(5) Determine the access requirements prior to requesting investigations for DOE contractor or subcontractor employees, consultants, or access permittees.

(6) Implement procedures which require DOE supervisors and DOE contractor organizations to report information received that an individual under their jurisdiction, possessing an active access authorization, is hospitalized or otherwise treated for a mental illness which may

cause a defect in judgment or reliability, and to notify DP-34 of this fact and when such employee is found to be free of such defect.

(7) Arranges for the service of a psychiatrist to examine an individual when such an examination is determined appropriate in resolving a question of eligibility for access authorization, or continuing access authorization.

(8) Implements procedures to assure that DOE supervisors and DOE contractor organizations are aware that:

(a) Information concerning an individual possessing an active DOE access authorization (or in process for same) that is a matter of personnel security interest should be reported to a DOE security official.

(b) Established reporting channels should be used in communicating a matter of personnel security concern to the appropriate DOE security official.

(9) Requests approval of DP-34 to initiate security investigations relative to foreign nationals.

(10) Refers to DP-34 requests for access authorization for employees of other Federal Departments and Agencies.

(11) Furnishes DP-34 with:

(a) Written notifications of withdrawals of requests for access authorization.

(b) An annual compilation of "positions of a high degree of importance or sensitivity" for certification.

(c) Data Reports on Spouse (DOE Form DP-354) for personnel under their jurisdiction who marry subsequent to the processing for an access authorization.

(12) Accepts for access to "Confidential" or "Secret" National Security Information or Formerly Restricted Data involved in DOE contracts and subcontracts, written assurances that personnel of the facility engaged in DOE work possess final Department of Defense or National Aeronautics and Space Administration (NASA) clearances for access to National Security Information and the type of investigation of which such clearances were granted. The written assurance shall be indicated on a DOE Form 5631.20; for NASA-cleared individuals a NASA Form 405 may be substituted. Clearances granted by Department of Defense contractors and interim "Confidential" or "Secret" clearances are not acceptable. Appropriate records of accepted clearances shall be maintained by the field organization.

(13) Generates requests to the Secretary or the Assistant Secretary for Defense Programs (DP-1), through DP-34, for interim access authorizations.

(14) Generates requests to the Secretary of Energy (through MA-20) for waivers of preappointment full field investigation requirement for candidates under consideration to occupy criticalsensitive positions.

(15) In addition to the above, managers of operations offices shall:

(a) Grant access authorization in all cases except those requiring processing for a hearing before a Hearing Officer.

(b) Cause individuals to be interviewed when the reported information falls within the criteria of 10 CFR Part 710 or Executive Order 10450.

(c) In connection with cases processed in accordance with 10 CFR Part 710.20 et seq., perform those functions assigned to the manager of the operations office.

(d) Extend, accept for transfer, reinstate, and terminate access authorizations as appropriate.

(e) Authorize transfer of contractor personnel, whose access authorizations are based upon investigations by the Office of Personnel Management or other Government agencies, to positions of a "high degree of importance or sensitivity" prior to receipt of Federal Bureau of Investigation reports.

(f) Furnish DP-34 with appropriate notifications of all access authorization actions.

(g) Approve and maintain records of review of personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.

(h) Accept investigations and reports on the character, associations, and loyalty of individuals made by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individuals by another Government agency based on such investigations and reports.

(i) Maintain personnel security files, as appropriate, containing copies of reports of investigation and other pertinent data on individuals granted a DOE security clearance by that office, or where an investigation was requested by that office and reports of investigation forwarded by virtue of the fact that the individual occupied a Critical-Sensitive position.

(j) Assure that the information reflected on standard employment forms completed by DOE employees, applicants for employment, consultants and assignees is comparable with the information reflected on security forms prior to the security forms being forwarded to the appropriate investigative agency.

(k) Evaluate all applicable reports of investigation conducted on DOE employees and applicants for employment under their jurisdiction for suitability in sensitive positions and notify the cognizant office of the results of each investigation for appropriate action.

(l) Arrange with other managers of operations offices for the performance of administrative services, under the provisions of this Order, when the location of a facility or individual is such as to justify such arrangement as a matter of convenience or economy.

LEVELS OF ACCESS FOR EACH CATEGORY OF CLEARANCE

Type Clearance

DOE employees, applicants for employment, consultants, and assignees; and DOE contractor and subcontractor employees and consultants:

"Q"-Sensitive (Badge is coded "1" or "2")	Top Secret Restricted Data, Formerly Restricted Data, and National Security Information; Secret Restricted Data, Formerly Restricted Data, and National Security Information; Confidential Restricted Data, Formerly Restricted Data, and National Security Information
"Q"-Nonsensitive (Badge is coded "3")	Top Secret National Security Information and Formerly Restricted Data; Secret Restricted Data, Formerly Restricted Data, and National Security Information; Confidential Restricted Data, National Security Information, and Formerly Restricted Data
Top Secret (Badge is coded "4")	Top Secret National Security Information and Formerly Restricted Data; Secret National Security Information and Formerly Restricted Data; Confidential National Security Information and Formerly Restricted Data
"L" (Badge is coded "5")	Secret National Security Information and Formerly Restricted Data; Confidential Restricted Data, Formerly Restricted Data, and National Security Information
Secret (Badge is coded "6")	Secret National Security Information and Formerly Restricted Data; Confidential National Security Information and Formerly Restricted Data

---

Employees of DOE access permit holders:

"Q(X)"	Secret Restricted Data; Confidential Restricted Data (as specified in the access permit)

"L(X)"	Confidential Restricted Data (as specified in the access permit)

Other Federal Department/Agency employees:

[illegible]"-Sensitive	Top Secret Restricted Data; Secret Restricted Data; Confidential Restricted Data
"Q"-Nonsensitive	Secret Restricted Data; Confidential Restricted Data
"L"	Confidential Restricted Data

TABLE OF CONTENTS

CHAPTER I - GENERAL GUIDELINES FOR POSITION SENSITIVITY DESIGNATIONS AND ACCESS AUTHORIZATIONS

1. General I-1
2. Position Sensitivity Determinations I-1
3. Access Level Determinations I-2
    a. Criteria for Determining Level of Access for DOE Employees, Consultants, and Assignees I-2
    b. Criteria for Determining Level of Access for DOE Contractor and Subcontractor Employees and Consultants and Access Permittees. I-3
    c. Other Federal Department or Agency Employees I-4
4. Sensitive Compartmented Information I-4

CHAPTER II - PROCESSING PERSONNEL SECURITY CASES

1. General II-1
2. Preparing the Request II-1
3. Investigative Requirements for Access Authorizations II-3
4. Prescreening of Personnel Security Cases II-4
5. DOE Personnel Security File Numbers II-4
6. Processing the Forms Used to Request Investigations II-4
7. Request for Investigation II-6
8. Access Authorization for other Federal Agency Employees II-7
9. DOE and DOE Contractor Personnel Assigned for Duty with DOE or NASA II-7
10. Additional Requirements for Investigation for U.S. Citizens Who Have Resided in Foreign Countries II-7
11. Transmittal of Investigative Reports Upon Completion II-8
12. Cancellation of Requests for Access Authorization or Investigation II-8
13. Requests for Copies of Missing Reports II-9
14. Types of Investigations II-9
    a. Federal Bureau of Investigation II-9
    b. Office of Personnel Management II-10
    c. Other Federal Agencies II-11
    d. Incomplete II-11
    e. When the NAC is Derogatory II-12
15. Transfers to "Positions of a High Degree of Importance or Sensitivity" II-12
16. Requesting Expedite Investigations II-13
17. Documentation Required in Granting Access Authorizations II-13
18. Reopening Cases II-13
19. DOE Custody of Investigative Reports II-14
20. Notification of Access Authorization Determination II-15
21. Arrangement of Data in Personnel Security Files II-15
22. Contents of Personnel Security Files II-16

Attachment II-1 .... II-17

CHAPTER III - SCREENING AND ANALYSIS OF PERSONNEL SECURITY CASES AND METHODS FOR DETERMINING ACCESS AUTHORIZATION ELIGIBILITY

1. Screening III-1
2. Analysis III-1
3. Referral of Cases for Advice III-2
4. Actions Authorized by the Office of Safeguards and Security III-2
5. Interviews III-3
6. Interrogatories III-3
7. Additional Investigations III-3
8. Special Updates III-3
9. Administrative Review Procedure III-3
10. Persons Treated for Mental Illness III-6
11. Disclosure of Reported Information III-7
12. Time Element in Processing Cases III-7

CHAPTER IV - INTERIM ACCESS AUTHORIZATIONS AND WAIVERS OF PREAPPOINTMENT FULL FIELD INVESTIGATIONS

1. General IV-1
2. Interim Access Authorization to Restricted Data IV-1
3. Interim Access Authorization to National Security Information IV-1
4. Waiver of Preappointment Full Field Investigation IV-2
5. Standards and Procedures IV-3

CHAPTER V - DATA ON SPOUSES

1. General V-1
2. Procedures V-1
3. Additional Requirements V-2

CHAPTER VI - ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS AND INDIVIDUALS POSSESSING DUAL CITIZENSHIP

1. Requirements VI-1
2. Standards and Procedures VI-1
3. Dual Citizenship VI-4

CHAPTER VII - EXTENSIONS, TRANSFERS, TERMINATIONS AND REINSTATEMENTS OF ACCESS AUTHORIZATIONS

1. Extensions and Transfers VII-1
2. Terminations VII-2
3. Reinstatements VII-4
4. Transmittal of Personnel Security Files VII-5

CHAPTER VIII - SELECTIVE REINVESTIGATION PROGRAM

1. General Information VIII-1
2. Reevaluation VIII-1
3. Determining the Type of Reinvestigation to be Conducted VIII-1
4. Scheduling Reinvestigations VIII-2
5. Evaluation Procedures VIII-2

CHAPTER IX - ESTIMATES OF REQUESTS FOR SECURITY INVESTIGATIONS

1. General IX-1
2. Procedures IX-1
3. Records IX-1

CHAPTER I

GENERAL GUIDELINES FOR POSITION SENSITIVITY DESIGNATIONS AND ACCESS AUTHORIZATIONS

1. GENERAL. Requests for investigation shall be submitted only after a determination has been made relative to (a) position sensitivity (Federal employees, applicants for Federal employment, consultants, and assignees only (see Federal Personnel Manual (FPM) 731, Subchapter 2, Appendix A)), and/or (b) that the duties of a position require access to classified information or special nuclear material in category I or II quantities, or regular access to a security area. Clearances are not to be requested as a means of alleviating individual or management responsibilities to properly safeguard classified information, control dissemination of such classified information on a "need-to-know" basis, or to preclude the use of access controls or physical barriers to distinguish between classified and unclassified areas or facilities. It is the intent of this policy to assure that clearances are granted only when absolutely required and at the level of access required, to avoid the unnecessary expenditure of agency funds and resources or the unwarranted invasion of an individual's right to privacy.

    a. The DOE will take all reasonable measures to obtain existing reports of investigation which may fulfill the agency standards and specifications as to the scope and extent of investigations established by the Secretary.

    b. Requests for clearances shall not be processed: (a) unless all required security forms are completed and signed (when appropriate) by the applicant and/or sponsor; (b) if the printed content of the security forms has been altered; (c) if insufficient, incorrect, or conflicting information is provided or the forms are illegible.

    c. The use of interim access authorizations shall be kept to the absolute minimum and considered only when properly requested in accordance with Chapter IV.

    d. The invocation of Section 145b (Atomic Energy Act of 1954, as amended) determinations for access to Restricted Data may be used only for Federal judges and justices, members of congress, and governors and Lt. governors.

    e. Updated security forms may be requested by DOE security officials at any time in order to update an individual's personnel security file.

2. POSITION SENSITIVITY DETERMINATIONS FOR DEPARTMENT OF ENERGY EMPLOYEES, APPLICANTS FOR EMPLOYMENT, CONSULTANTS, AND ASSIGNEES ONLY.

    a. Position sensitivity determinations shall be made by the responsible managers of operations offices (or their designees) or the responsible

Heads of Headquarters Elements, as outlined in the FPM Chapter 731, Subchapter 2, Appendix A.

b. Investigation Requirements Based on Position Sensitivity for Department of Energy (DOE) Employees, Applicants for Employment, Consultants, and Assignees:

Position Sensitivity	Investigative Requirements
Special-Sensitive	Special Background Investigation
Critical-Sensitive	Background Investigation
Noncritical-Sensitive	Limited Background Investigation
Non-Sensitive	National Agency Check and Inquiries

3. ACCESS LEVEL DETERMINATIONS. To assure that investigative coverage is appropriate for the access required for a position, a determination shall be made as to what type of classified information, special nuclear material, or special security areas are required by each position and certified in writing to the Director of Safeguards and Security (DP-34), or to the DOE official at a DOE field office. The following criteria shall be used in the determination of access level. (NOTE: For Federal employees, applicants for Federal employment, consultants and assignees, there is no direct relationship between position sensitivity and level of access to classified information, special nuclear materials, or security areas.)

a. Criteria for Determining Level of Access for DOE Employees, Consultants, and Assignees.

(1) "Q" Sensitive. The following responsibilities or consideration shall be used to establish whether a particular position is to be designated a "position of a high degree of importance or sensitivity" ("Q" sensitive access authorization) within the meaning of Section 145f of the Atomic Energy Act of 1954, as amended, requiring that the investigation be conducted by the Federal Bureau of Investigation.

(a) Regular access to Top Secret Restricted Data.

(b) Regular access to Restricted Data involving broad policy or program direction, and this position may affect such policy direction, in any of the following:

1 Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.

2 Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.

3 Research, development, or production in the laser fusion or laser isotope programs.

4 Naval nuclear propulsion program.

(2) "Q" Nonsensitive. The following considerations shall be used to establish whether a particular position requires a "Q" nonsensitive access authorization:

(a) Access to Secret Restricted Data.

(b) Access to special nuclear material in categories I and II.

(3) Top Secret. The following considerations shall be used to establish whether a particular position requires a Top Secret access authorization:

(a) Access to Top Secret National Security Information.

(b) Access to, and development of war plans or particulars of future or major or special operations of war, or critical or extremely important items of war.

(4) "L."

(a) Access to Confidential Restricted Data.

(5) Secret.

(a) Access to Secret or Confidential National Security Information.

b. Criteria for Determining Level of Access for DOE Contractor and Subcontractor Employees and Consultants and Access Permittees.

(1) To assure that investigative coverage is appropriate, the individual's type of access (Restricted Data, National Security Information, or unclassified special nuclear material in category I or II quantities) and level of access (Top Secret, Secret, or Confidential) shall be determined, using the criteria on pages I-2 and I-3, paragraphs 3a(2) through 3a(5), before a request for investigation is made by the appropriate DOE official. Additionally, a DOE contractor or subcontractor employee or consultant position shall be designated as a "position of a high degree of importance or sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position fall within the scope on page I-2, paragraph 3a(1).

(2) It is DOE policy not to establish a separate clearance program for DOE contractor and subcontractor employees and consultants and access permittees for positions associated with unclassified Federal computer systems. Rather, the contractor, subcontractor, consultants, or access permittee is responsible for maintaining satisfactory standards of employees' qualifications, performance, conduct, and business ethics under its own personnel policies (U.S. Department of Energy Procurement Regulation, Subpart 970.2201, "Basic Labor Relations").

c. Other Federal Department or Agency Employees, Legislative and Judicial Branch Employees:

(1) DOE will withhold the access to Restricted Data, Formerly Restricted Data, or National Security Information under DOE responsibility, and quantities of special nuclear material to other Federal department or agency employees, and Legislative, and Judicial Branch employees until the DOE has made a determination that such access shall not endanger the common defense and security. Except as authorized by the Secretary or his designee that such action is clearly consistent with the national security, this determination shall be based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another government agency which conducts personnel security investigations provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individual based on such investigation and report.

(2) Additionally, positions within other Federal agencies (exclusive of personnel of the Department of Defense and the National Aeronautics and Space Administration, who do not require DOE security clearance by virtue of Section 143 of the Atomic Energy Act of 1954, as amended, or Section 304(b) of the National Aeronautics and Space Act of 1958) and agencies shall be designated as a "position of a high degree of importance or sensitivity" within the meaning of Section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position fall within the scope on page I-4, paragraph 3c(1).

4. SENSITIVE COMPARTMENTED INFORMATION (SCI). Within the DOE, determination concerning an individual's eligibility for access to SCI is the responsibility of the DOE Senior Official of the Intelligence Community (SOIC) and his/her designated representative(s). The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in Director of Central Intelligence Directive (DCID) No. 1/14. The DOE will approve only DOE and DOE contractor employees for access to SCI.

CHAPTER II

PROCESSING PERSONNEL SECURITY CASES

1. GENERAL. This chapter covers the procedures for initiating and processing requests for full field investigations, National Agency Checks and Inquiries (NACI), and National Agency Checks (NAC), required for access authorizations, and for DOE employees employed in Special-Sensitive, Critical Sensitive and Noncritical-Sensitive positions.

2. PREPARING THE REQUEST.

   a. Before a request for investigation or access authorization is submitted, the following determinations should be made:

      (1) The level of access authorization required (guidelines contained in Chapter I).

      (2) The position sensitivity (required for DOE employees and consultants only). For guidelines in making this determination, refer to Federal Personnel Manual Chapter 731, subchapter 2, "Position Sensitivity."

      (3) Whether the individual has previously been granted access authorization by the DOE which can be reinstated, transferred, or extended.

      (4) Whether the individual has been granted a security clearance by another Government agency, and if so, all available information relating to such clearance (date, place, level, whether active or terminated, etc).

      (5) Whether the individual is a foreign national or dual citizen requiring Headquarters approval prior to processing for investigation (see Chapter V).

   b. Types of access authorizations and forms required to process. The following list shows the minimum forms required by the OPM and FBI to conduct investigations. Individual personnel and security offices may have additional requirements to process these requests.

      (1) DOE employees and DOE consultants

         (a) "Q" Sensitive that has been designated as a "Position of a High Degree of Importance or Sensitivity" using guidelines contained on page I-2, paragraph 3a(1).
         DOE Form DP-1, Personnel Security Questionnaire (PSQ),
           Part I and II, original and 5 copies.
         DOE Form 5631.18, Security Acknowledgement, 1 copy.
         FD-258, FBI Fingerprint Card, 2 copies.
         DOE Form 5637.1, Authority to Release Information, 1 copy.

(b) "Q" Sensitive, "Q" Nonsensitive, or "Special-Sensitive No Access"
DOE Form DP-1, Personnel Security Questionnaire, Part I and II, an original and 5 copies.
DOE Form 5631.18, Security Acknowledgement, 1 copy.
SF-87, OPM Fingerprint Card, 2 copies.
DOE Form 5637.1, Authority to Release Information, 1 copy.

(c) "Top Secret," or "Critical-Sensitive no Access"
SF-86, Security Investigation Data for Sensitive Position an original and 5 copies.
DOE Form 5631.18, Security Acknowledgement, 1 copy for "Top Secret" only.
SF-87, OPM Fingerprint Card, 2 copies.
DOE Form 5637.1, Authority to Release Information, 1 copy.

(d) "L"
DOE Form DP-1, Personnel Security Questionnaire, Parts I and II, an original and 5 copies.
DOE Form 5631.18, Security Acknowledgement, 1 copy.
SF-87, OPM Fingerprint Card, 2 copies.
SF-85-A, National Agency Check of Data for Nonsensitive or Noncritical-Sensitive position.

(e) "Secret"
SF-85, Data for Non-Sensitive or Noncritical-Sensitive Position, an original and 2 copies.
DOE Form 5631.18, Security Acknowledgement, 1 copy.
SF-87, OPM Fingerprint Card, 2 copies.
SF-171, Personnel Qualifications Statement, 1 copy.

(f) "Noncritical-Sensitive," or "Non-Sensitive" with no access to classified information
(The investigation that is required for employees in these categories will be processed through the Office of Personnel.)
SF-85, Data for Nonsensitive or Noncritical-Sensitive position, original and 2 copies.
SF-87, OPM Fingerprint Card, 2 copies.
SF-171, Personnel Qualifications Statement, 1 copy.

(2) DOE contractor employees, subcontractor employees, and their consultants.

(a) For all levels of access authorization:
DOE Form DP-1, Personnel Security Questionnaire, Parts I and II, an original and 5 copies.
DOE Form 5631.18, Security Acknowledgement, 1 copy.
FD-258, FBI Fingerprint Card, 2 copies.

Plus the following forms:

(b) "Q" Sensitive, "Q" Non-Sensitive and "Top Secret" only:
DOE Form 5637.1, Authority to Release Information, 1 copy.

(c) "L" and "Secret" only:
SF-85-A, National Agency Check of Data for Nonsensitive or Noncritical-Sensitive position.

(3) Other Government agency employees, (including Congressional and Judicial staff members), consultants and contractor employees may be processed for "Q" Sensitive, "Q" Nonsensitive, and "L" access authorizations, and will require the same forms as listed on page II-1, paragraph 2b(1).

(4) Employees of DOE access permit holders, "QX" and "LX".
DOE Form DP-1, Personnel Security Questionnaire, Part I and II, an original and 5 copies.
DOE Form 5631.18, Security Acknowledgement, 1 copy.
FD-258, FBI Fingerprint Card, 2 copies.
For "QX" only include DOE Form 5637.1, Authority to Release Information, 1 copy.

3. INVESTIGATIVE REQUIREMENTS FOR ACCESS AUTHORIZATIONS. Investigations are required for the access authorization levels as indicated below:

a. "Q" Sensitive - Full field investigation that covers at least the most recent 15 years. This shall require either a full field background investigation by the FBI, or a special background investigation by OPM. If the position has been designated as being of a "High Degree of Importance or Sensitivity," the investigation is done by the FBI. Persons under 18 years of age may not be processed for an FBI full field investigation, but should be submitted for background investigation by OPM.

b. "Q" Nonsensitive, "Top Secret," and "QX" - OPM full field background investigation. When a "QL" is requested, the National Agency Check Check portion of the investigation shall be returned in advance of the full field investigation and an "L" access authorization can be granted if appropriate, pending completion and review of the full field. These levels of access authorization may also be based upon full field investigation by a Government agency other than the FBI or OPM which conducts personnel security investigations, provided that a security clearance has been granted to the individual by such agency based on such investigation and report.

c. "L", "Secret," and "LX" - OPM National Agency Check and Inquiry with credit check for Federal employees; OPM National Agency Check with credit check for non-Federal employees.

d. "QB" - None required. This is an access authorization granted by the Assistant Secretary for Defense Programs, pursuant to Section 145b of the Atomic Energy Act of 1954, as amended, when it has been determined that such action is clearly consistent with the national interest. This authority cannot be redelegated. A "QB" access authorization will normally be processed only for members of Congress, Federal justices and judges, and, at the request of field office Managers of Operations, for appropriate elected State officials. A "QB" access authorization precludes the conduct of a background investigation, and, therefore, shall not be requested when an interim access authorization is appropriate, or when an investigative report exists which may be used as a basis for an access authorization.

e. In addition, a full field investigation is required for DOE employees in Critical-Sensitive positions, even if access to classified matter is not necessary. Each DOE employee in a Noncritical-Sensitive or nonsensitive position shall be processed for a National Agency Check and Inquiry (NACI), as a minimum, according to the requirements of the Federal Personnel Manual, which are implemented by this Order. Guidelines are contained in Chapter I as to whether a NACI is to be processed and adjudicated prior to or after an individual's appointment to Federal Service.

4. PRESCREENING OF PERSONNEL SECURITY CASES.

a. Personnel Security cases shall be prescreened by the requesting DOE security office to assure that:

(1) All information, including the proper forms for a full and timely investigation is made available to the investigative agency.

(2) Cases in which the PSQ, SF-86, SF-85, or SF-171 reflect omissions or discrepancies have been corrected.

(3) Contractors are conducting adequate preemployment checks prior to requesting access authorization in accordance with DOE procurement regulations.

5. DOE PERSONNEL SECURITY FILE NUMBERS. DOE personnel security file numbers will be assigned consecutively, by the appropriate security office, as individuals are initially processed for access authorizations: "Q," "Top Secret," "L," or "Secret," and for applicants processed under the Access Permit Program. Once assigned, a DOE personnel security file number shall continue to be used for identifying that individual's file, regardless of the field office location of that file.

6. PROCESSING THE FORMS USED TO REQUEST INVESTIGATIONS.

a. A Personnel Security Questionnaire (DOE Form DP-1), SF-86, or SF-85, will be used in requesting National Agency Checks, National Agency Checks and Inquiries, and full field investigations, or initiating reinvestigations or reinstatements. The form submitted should be legible, completely filled out, and based on information furnished by the individual. Part I of the DP-1 must be typed. A copy of the completely executed DP-1, SF-86, or SF-85 shall be retained by the DOE Security Office submitting the request. If the DP-1 is used, four copies shall be submitted to the investigative agency. If the SF-85 or SF-86 are used, two copies shall be forwarded. If the SF-85-A is required, he original, which must be typed, should be submitted with the request. The type of access authorization requested shall be stamped in the upper righthand corner of each copy of the DP-1, SF-85, or SF-86. The symbol of the office submitting the forms shall be used as a suffix if it differs from the original DOE file number. No more than 60 days shall elapse between the date of execution of the DP-1, SF-85, SF-86, or Authority for Release of Information, and its submission to the investigative agency. Forms that are more than 60 days old shall be returned to the individual for updating and resigning.

b. Fingerprint Cards, SF-87, shall be used in cases involving Federal employees being processed for OPM investigations. In all other cases, the FD-258 will be used. The DOE Security File number should be inserted in the "Number" space on the FD-258, and listed on the bottom of the "Title and Address" section of the SF-87. The type of access authorization requested as indicated on page II-1, paragraph 2, can be stamped in either the block entitled "Reason Fingerprinted" or "Title and Address." "U.S. Department of Energy, Washington, D.C." will be typed in the block entitled "ORI" where this has not already been overprinted on the FD-258.

(1) It is essential that the personnel assigned to take fingerprints be adequately trained to recognize unclassifiable prints and to assure that such prints are not submitted. Fingerprint cards that cannot be classified by the FBI cause undue delay in the clearance determination process. In the event that fingerprint cards are returned by the FBI as "unclassifiable," it is important that in making retakes particular care is observed to assure that the resubmissions are classifiable.

(2) When submitting fingerprint retakes, the unclassifiable fingerprint card (i.e., previously submitted and rejected as "illegible") should be attached to the new cards, with a cover letter indicating the type of investigation and access authorization that has been requested for the individual. It is particularly important to assure when submitting retakes to the OPM, that the OPM serial number is clearly indicated on the previously rejected fingerprint cards attached to the new retakes.

(3) Fingerprint retakes for individuals being processed for OPM full field investigations shall be forwarded to the following address:

U. S. Office of Personnel Management
Office of Personnel Investigations
P. O. Box 886
Washington, DC 20044

(4) Fingerprint retakes for individuals being processed for OPM National Agency Checks or National Agency Checks and Inquiries shall be forwarded forwarded to the following address:

U. S. Office of Personnel Management
Personnel Investigations Division
NACI Center
Boyers, PA 16018

(5) Fingerprint retakes for individuals being processed for FBI investigations shall be submitted to the following address:

Federal Bureau of Investigation
U. S. Department of Justice
ATTN: Identification Division
Washington, DC 20535

c. Authority to Release Information (DOE Form 5637.1) shall be forwarded to the investigative agency in all cases where a full field investigation is requested.

d. File Summary Sheet (DOE Form 5631.16) shall be prepared and placed in the personnel security file of the individual.

e. Transmittal Jacket. The DP-1, SF-85, or SF-86, SF-85A, fingerprint cards, and Authority to Release Information, if applicable, shall be enclosed in a transmittal jacket or envelope which lists on the outside the full name, the DOE file number, and the type of access authorization requested.

7. REQUEST FOR INVESTIGATION.

a. The security forms being submitted to the FBI or OPM shall be accompanied by one "Request for Investigation," described below, which may include the names of several individuals provided all requests are of the same type.

b. DOE Form DP-5631.24 shall be used inforwarding request for FBI investigation. While several names may be indicated on the DOE Form 5631.24, the FBI requires one copy of the form for each name listed on the DP-5631.24. A copy should be made for retention in the individual's personnel security file.

c. One copy of DOE Form DP-5631.23 shall be used in forwarding requests for OPM investigations. A copy should be made for retention in the individual's personnel security file.

8. ACCESS AUTHORIZATION FOR OTHER FEDERAL AGENCY EMPLOYEES. All requests for access authorization of employees of other Federal agencies or departments and their contractors shall be processed through the Director, Division of Security, Headquarters. Personnel of Department of Defense and National Aeronautics and Space Administration may have access to Restricted Data under the certification procedures outlined in DOE Order 5631.5, "Control of Classified Visits," except in those cases indicated below.

a. DOD and NASA Personnel Assigned for Duty with the DOE. These individuals shall require DOE access authorization and shall in their assigned capacity be afforded access to Restricted Data on the same basis as DOE employees. When the situation warrants, they may be assigned for duty on the basis of an appropriate certification of clearance from their agency, providing the processing for DOE access authorization has been initiated. Restricted Data received by such personnel during their assignment with DOE must be handled in accordance with DOE security regulations.

b. DOD and NASA Personnel Assigned for Duty with Other Federal Agencies. When these individuals shall require DOE access authorization, the requests must be initiated by the agency to which they are assigned.

9. DOE AND DOE CONTRACTOR PERSONNEL ASSIGNED FOR DUTY WITH DOD OR NASA. Any DOE or DOE contractor employee acting as a consultant or member of an advisory board of DOD or NASA who in that capacity possesses appropriate Department of Defense (DOD) or National Aeronautics and Space Administration (NASA) clearance, shall for the purposes of this part, be considered as a temporary employee of DOD or NASA. In this capacity he/she may communicate Restricted Data to personnel of DOD or NASA and their contractors in accordance with the security regulations of DOD or NASA. In the event the DOE employee or contractor does not require a clearance or access authorization for their DOE work, but does require a clearance for their assignment to the other agency, it shall be the responsibility of the other agency, rather than DOE, to request the appropriate investigation.

10. ADDITIONAL REQUIREMENTS FOR INVESTIGATION OF U.S. CITIZENS WHO HAVE RESIDED IN FOREIGN COUNTRIES, INCLUDING THOSE WHO HAVE BEEN RECENTLY NATURALIZED.

The investigative history of these types of cases has indicated that coverage may be obtained only in Canada and the United Kingdom, or in such places as West Germany where the U. S. Armed Forces are represented. Beyond this, State Department records checks made by the U. S. Embassy in a particular country are usually all that may be anticipated, and in some countries even this may not be possible.

Consequently, in order to comply with section 145 of the Atomic Energy Act of 1954, as amended, and Executive Order 10450, investigative agencies must rely on leads in the United States to produce sufficient investigation on which a determination can be made as to an individual's eligibility for access authorization.

a. In cases where it appears likely that adequate investigation is obtainable on which to predicate a determination of eligibility for access authorization, the supplemental information outlined on page II-17, Attachment II-1, "Additional Information to be Obtained for Individuals Who Have Resided in Foreign Countries" shall be furnished by the applicant. This shall be submitted to the investigative agency in quadruplicate with the completed Personnel Security Questionnaire, or SF-86.

b. If, upon review of the PSQ, or SF-86 by the DOE security office, it appears unlikely that adequate investigation can be obtained, all material pertaining to the case shall be forwarded to the Office of Safeguards and Security, Headquarters, for discussion with the investigative agencies (Department of State, Immigration and Naturalization Service and other Federal agencies), as appropriate. The Office of Safeguards and Security, Headquarters, shall then advise as to whether sufficient investigation can be obtained on which a determination can be made as to the individual's eligibility for access authorization. In cases where the individual has resided in, or has relatives living in a country where the language is written in a non-Roman alphabet (i.e. Hebrew, Arabic, Chinese, Japanese, Russian, etc.), the individual should be requested to furnish the identifying information on former overseas addresses and on relatives written in the other alphabet.

11. TRANSMITTAL OF INVESTIGATIVE REPORTS UPON COMPLETION. The OPM forwards reports of full field investigation and the results of National Agency Checks with Credit and National Agency Checks and Inquiries directly to the requesting office. Completed FBI Investigations are sent to the Office of Safeguards and Security, Headquarters. The documents are then transmitted to the appropriate field office. Upon receipt of the reports, each field office shall enter the date the reports were received into the Central Personnel Clearance Index (CPCI) following instructions contained in the CPCI system reference manual.

12. CANCELLATION OF REQUESTS FOR ACCESS AUTHORIZATION OR INVESTIGATION.

a. Cancellation prior to completion of investigation. When a request for access authorization or investigation of an individual is withdrawn prior to completion of the investigation or National Agency Check, the Office of Safeguards and Security, Headquarters, shall be notified immediately by telephone so that the investigation may be discontinued. This call shall be followed-up with a teletype message containing the full name of the individual, the DOE security file number, the name of the investigative agency and the date and type of request being cancelled ("Q," "Top Secret," "L," "Secret," or "Critical-Sensitive/No Access"). The Office of Safeguards and Security, Headquarters, shall immediately request the investigative agency by telephone to discontinue the investigation and for FBI cases shall confirm this request by letter, forwarding a copy to the interested field office. The field office shall enter this cancellation information into the the CPCI following instructions contained in the CPCI System Reference Manual.

b. By agreement with the FBI and OPM, the DOE shall be charged for the investigation if any field investigation has been conducted. However, if a case for which DOE has been billed is resubmitted for investigation within one year, there shall be no additional charge.

c. Cancellation after completion of investigation. When a request for access authorization is cancelled or withdrawn after completion of the investigation, but prior to granting of access authorization, the cognizant DOE office shall enter this information into the CPCI.

d. Cancellation of request for reinvestigation. When an individual terminates employment, or the need for access authorization no longer exists, the Manager of Operations or for Headquarters cases (including Regional employees), the Office of Personnel or the contract officer will notify the Office of Safeguards and Security, Headquarters, immediately by telephone, so that the reinvestigation may be discontinued. This call shall be followed up with a teletype memorandum to verify the cancellation. Such names may be included on messages concerning applicant type investigations providing the individuals are identified as "reinvestigation" cases. In addition, two separate actions must be taken to update the CPCI: The current, active clearance must be terminated and the pending reinvestigation must be closed out either by a deletion or by evaluation of the reports and submission of the results to CPCI.

13. REQUESTS FOR COPIES OF MISSING REPORTS. Requests for copies of missing reports shall be made by memorandum to the Office of Safeguards and Security, Headquarters, for processing to the OPM or FBI. Each request shall be accompanied by a copy of the PSQ, SF-85, or SF-86 which served as the basis for the investigation. Upon receipt of copies of the missing reports, they shall be forwarded to the requesting office by the Office of Safeguards and Security, Headquarters, together with the PSQ, SF-85, or SF-86.

14. TYPES OF INVESTIGATIONS.

a. Federal Bureau of Investigation (FBI).

(1) Background investigation. This type of investigation involves coverage of the individual's adult life since his or her 18th birthday. It includes personal contact of the individual's

references, and at the individual's present and all past residences and employments, and education during the most recent 5 years. Records shall be checked for all military service, periods of higher education (or high school if the individual has had no higher education), police departments and credit bureaus at all places of residences and employment during the most recent 15 years or since the individual's 18th birthday, embassies for all periods of overseas residence (plus State Department investigation if possible), and at Bureau of Vital Statistics if inconsistencies develop regarding the individual's name, or date and place of birth. A name check shall also be conducted with the FBI's criminal and subversive files, the OPM Security Investigations Index, Defense Central Index of Investigations (DCII), and for foreign born individuals or spouses, Central Intelligence Agency (CIA) and Immigration and Naturalization Service (INS). CIA shall also be checked if extensive foreign travel has been indicated. A fingerprint check through the FBI's Identification Division shall complete this investigation.

(2) File and Fingerprint Check. This shall consist of a fingerprint check through the FBI's Identification Division, as well as a name check through the FBI's criminal and subversive files.

b. Office of Personnel Management (OPM).

(1) National Agency Check with Credit (NACC). A NACC consists of a records check of the individual's name with the FBI's criminal and subversive files, OPM's Security Investigations Index, DCII (whenever military or civilian Department of Defense (DOD) or DOD prime contractor employment is indicated), INS (whenever U.S. citizenship by other than birth is indicated), and CIA (whenever extensive foreign travel is indicated). A fingerprint check shall also be made through the FBI's Identification Division. A credit check shall also be conducted in connection with a NACC.

(2) National Agency Check and Inquiry (NACI). A NACI includes the checks conducted for a NAC as indicated on page II-10, paragraph 14b(1), plus written inquiries are sent to the individual's supervisor at places of employment during the most recent 5 years, police departments having jurisdiction over the individual's residences during the most recent 5 years, all education where the individual received a degree relating to the position applied for, all education during the most recent 5 years, and listed references. A credit check may also be conducted in connection with a NACC.

(3) Minimum Background Investigation (MBI). The MBI consists of the NACI described on page II-10, paragraph 14b(2), and a credit search. Telephone inquiries are made whenever the initial written inquiries are not returned, to insure that adequate coverage is obtained.

(4) Limited Background Investigation (LBI). The LBI consists of a subject interview (if the subject is a Federal employee only), personal interviews with selected sources covering specific areas of subject's background during the most recent 1-3 years, and written inquiries and record searches for a total of 5 years.

(5) Background Investigation (BI). The BI consists of a subject interview (if the subject is a Federal employee only), written inquiries, record searches, credit search, and personal interviews with selected sources covering specific areas of the subject's background up to the past 7 years, but not less than 5 years.

(6) Special Background Investigation (SBI). The SBI consists of a subject interview (if the subject is a Federal employee only), written inquiries, record searches, credit search, and personal interviews with selected sources covering specific areas of the subject's background during the most recent 15 years.

c. Background Investigations by Other Federal Agencies. Reports of personnel security investigations by other Federal agencies may be accepted in lieu of reports by the Office of Personnel Management provided that the investigation meets the scope and extent of the OPM investigation and provided that a security clearance has been granted by another Federal agency based on such investigation and report.

d. Incomplete National Agency Checks. In order to expedite the processing of "Secret," "L," and "LX" access authorizations, the DOE accepts NACs from the OPM which are incomplete, provided the missing checks are clearly identified. The OPM has been advised that the checks from the FBI and OPM must be completed prior to submission to DOE. Upon receipt of such incomplete NAC's in field offices, managers may, when the situation so requires, grant "Secret," "L," or "LX" access authorization, provided that (as a minimum):

(1) A review of the PSQ's or other security forms and the checks received is favorable.

(2) The individual, his employer or prospective employer, furnishes satisfactory evidence to indicate that there were no adverse circumstances of a security nature surrounding the individual's military service (or employment) or foreign travel. Submission by the individual of his discharge papers or his passport, either directly to DOE, his employer or prospective employer, will ordinarily suffice for this purpose.

(3) A further review of the case shall be made when the incomplete checks are received.

e. Requests for full field investigation where National Agency Checks reveal derogatory information. When the National Agency Check discloses substantially derogatory information in relation to the DOE access authorization criteria, managers of field offices shall submit a request for a full field investigation to the Office of Personnel Management setting forth the reasons therefor accompanied by four copies of up-to-date Personnel Security Questionnaire (Form DP-1), and a fingerprint card if more than 6 months has elapsed since the request for National Agency Check was forwarded to the OPM, and a DOE Form DP-5637.1, Authority to Release Information.

15. REQUESTING FBI INVESTIGATION FOR INDIVIDUALS TRANSFERRED TO "POSITIONS OF A HIGH DEGREE OF IMPORTANCE OR SENSITIVITY."

a. When an individual, whose access authorization was based upon an investigation conducted by the Office of Personnel Management or other Government agency that conducts personnel security investigations, is being transferred to a position which has been certified by the Department as being a position of a "high degree of importance or sensitivity" (see Chapter I) a request for a full field investigation shall be forwarded to the FBI by the field office. If the individual being transferred has been the subject of a full field investigation by the OPM within the past 3 years, the Manager may authorize the transfer to the new position, provided the existing personnel security file is reviewed before the transfer takes place. In such cases, the individual shall be processed for an FBI reinvestigation when the existing investigation is 5 years old. The manager of the field office may also authorize the transfer to the new position prior to receipt of a completed FBI full field investigation, provided the existing personnel security file is reviewed before the transfer takes place.

In requesting this investigation, the FBI will be furnished with:

(1) A Request for Investigation (Form DP-5631.24).

(2) Four copies of an up-to-date PSQ (Form DP-1) which shall indicate that the position is of a "high degree of importance or sensitivity."

(3) A new fingerprint card.

(4) One copy of each of the reports of the previous investigation conducted by OPM or other Federal agency.

16. REQUESTING EXPEDITE INVESTIGATIONS. In instances where there is an emergency or critical need for the immediate services of an individual being processed for a full field investigation, the investigative agency can be requested to conduct the investigation on an expedited basis. The following procedures shall be followed in such cases:

   a. The field office requesting the expedited service shall forward a memorandum to the Chief, Personnel Clearance Branch, Headquarters. That memorandum must indicate the name, DOE file number, number and date of the "Request for Investigation" (DOE Form DP-5631.23 or DOE Form DP-5631.24), as well as justification for the expedited service.

   b. All copies of the paperwork being submitted to the investigative agency shall be stamped "EXPEDITE," at the time they are forwarded to OPM or the FBI.

   c. The Chief, Personnel Clearance Branch, Headquarters, shall review the request for expedited service, and if approved, shall make the necessary arrangements with the OPM or the FBI.

17. DOCUMENTATION REQUIRED IN GRANTING ACCESS AUTHORIZATIONS.

   a. When access authorization has been granted, the field office shall make the appropriate entry into the CPCI following instructions contained in the CPCI system reference manual.

   b. Process Index Cards (Form DP-222b) may be used to provide an alphabetical index of all individuals processed for access authorization.

18. REOPENING OF CASES IN WHICH REQUESTS FOR ACCESS AUTHORIZATION WERE CANCELLED.

   a. Full Field Investigations.

      (1) When a full field investigation, which was discontinued prior to completion, is again required, the field office shall request such action by forwarding a Request for Investigation (Form DP-5631.23 or 5631.24), to the appropriate agency. The Request for Investigation should be marked "Reopen Case" and the date of the previous request and cancellation should be indicated. The extent of reports previously received (e.g., NAC only, partial full field reports, etc.) will aid the investigative agency in rescheduling the case.

      (2) When the request for access authorization has been cancelled (not hired) after the completion of the investigation and updating of the investigation is deemed necessary, the procedure outlined on page II-13, paragraph 18a(1), shall be followed.

(3) If more than a year has elapsed or any significant changes are known to have occurred since the execution of the previous PSQ or SF-86, new forms, Authority to Release Information, and fingerprint cards shall be submitted.

b. Copies. If the original investigation was not made by the same investigative agency, one copy of each report of the previous investigation and new security forms shall be forwarded with the request. If no reports were received it shall be so indicated on the DP-5631.23 or 5631.24.

c. Reopening of reinvestigations previously conducted. When a reinvestigation which was discontinued prior to completion is again required, field offices shall request such action by forwarding a Request for Investigation (Form DP-5631.23 or 5631.24), to the FBI or OPM.

19. DOE CUSTODY OF INVESTIGATIVE REPORTS.

a. Because of the privileged nature of the information contained in the investigative reports and the personnel security files, they shall be made available only to authorized Government officials. Appropriate measures will be taken for their handling, transmission, and housing to assure that this requirement is carried out. Reports or information contained therein shall not be made available to contractors' representatives.

b. Availability of Investigative Reports to Other Agencies. Reports of investigation on individuals who have been processed for DOE access authorization may be exhibited to accredited representatives of the Armed Forces or other Federal agencies provided such representatives show that they have an official and legitimate interest in the information contained in the reports. Representatives shall not be given copies of the reports but shall be advised that they may be requested directly from the FBI, OPM, or other Federal agency. Representatives may also review copies of informal interviews and hearing transcripts, but shall not be provided copy(ies) unless the individual has authorized such release in writing. The release executed by the individual must explicitly refer to the interview and/or hearing transcript or summary contained in the DOE personnel security file. A copy of the release and a listing of the material released shall be maintained in the individual's DOE personnel security file. In addition, the procedures in the following paragraphs must be adhered to by DOE security officials.

c. In accordance with Public Law 93-579, 93rd Congress, S. 3418, December 31, 1974, "Privacy Act of 1974," an accounting shall be maintained of each disclosure of the contents of a DOE Personnel Security File to any other agency representative or other individual authorized to review the investigative reports, copies of informal interviews, and hearing transcripts. Prior to the physical review of the Personnel Security File, the following information shall be noted in the file:

(1) Name of the person to whom the disclosure is made.

(2) Agency represented and address.

(3) Date.

(4) Nature and purpose of the disclosure.

(5) Name of the DOE employee releasing the information.

d. Pursuant to Section 552a(b)(7) of the Privacy Act, no information relative to a civil or criminal enforcement activity is to be released unless the head of the requesting agency or department makes a written request specifying the portion desired and the law enforcement activity involved. Such requests should be directed to the Director, Office of Safeguards and Security, Headquarters or managers of field offices, as appropriate.

e. Prior to the release of personnel security files containing classified information, the DOE employee responsible for releasing the file shall be assured that the reviewer possesses the appropriate level of access authorization or clearance.

20. NOTIFICATION OF ACCESS AUTHORIZATION DETERMINATION. The determination made by the DOE to grant or deny access authorization shall be furnished in writing or orally with written confirmation to the employer, prospective employer or access permittee who initiated the request. This information may also be furnished to representatives of other DOE contractors, representatives of the Armed Forces or other Federal agencies having an official interest in the individual. Determinations to grant access authorization shall not be given in writing to the individual himself except:

a. In those cases in which the determination was made as a result of a completion of the DOE administrative review process as specified in 10 CFR Part 710.

b. Or when the individual is also the designated official in the agency, or in his firm or organization to whom written notifications are forwarded.

21. ARRANGEMENT OF DATA IN PERSONNEL SECURITY FILES.

a. To the right-hand side of the file folder shall be fastened the Personnel Security Questionnaire, SF-85's or SF-86's, fingerprint cards; FBI Forms

T-1, 1-C, T-2, 1-4, or other identification record; Security Acknowledgement forms; reports of investigation; letters or memoranda containing investigative data; and summaries of investigation or security statements arranged in chronological order beginning with the oldest document at the bottom. Only the top of the PSO shall be fastened in order that it can be readily opened for review.

b. To the left-hand side of the file folder shall be fastened memoranda and other correspondence relating to the administrative handling of the case arranged in chronological order.

c. Duplicate material shall be placed on the appropriate side of the file folder under a file separator marked "Duplicate Material." Duplicates shall be filed in the same order as the originals are filed above the separator.

22. CONTENTS OF PERSONNEL SECURITY FILES. In addition to the documents and investigative reports used to determine the individual's eligibility or continued eligibility for access authorization, the personnel security file of any individual who has been processed for DOE access authorization, whether active or terminated, shall contain the original or a copy of any correspondence or form involving the individual subsequent to the initial clearance action. Such material may include, but is not limited to:

a. Subsequent investigative reports (including informal reports or records of verbal reports) from any Government agency or local law enforcement activity concerning the individual, the DOE Office of the Inspector General, or from contractor security personnel.

b. Newspaper clippings, court records, or other information reflecting arrests or investigation for possible criminal activity on the part of the individual or spouse.

c. Data Report on Spouse (DOE F 5631.34) and investigative reports received on the spouse.

d. Records of security infractions and followup actions.

e. Transcripts of security interviews and/or "Release of Information" documents executed by the individual.

f. Foreign travel to Soviet Bloc countries.

g. Records of "Classified Visits/Access Approvals" or clearance certificates.

h. Special authorization for sensitive information, including Top Secret production, stockpile and Weapons Data, and Sensitive Compartmented Information.

i. Reports of hospitalization or treatment for mental illness.

j. DOE and NASA certifications for visits or access.

k. Security badge and briefing forms.

l. DOE "Letters of Interrogatory" to the individual and the individual's response to such letters.

ADDITIONAL INFORMATION TO BE OBTAINED FOR INVESTIGATION OF U.S. CITIZENS WHO HAVE RESIDED IN FOREIGN COUNTRIES

1. EMPLOYMENT. The names and addresses of individuals living in the United States who were associated with applicant in the foreign country as supervisor, employee, or fellow worker.

2. RESIDENCE. The names and addresses of individuals living in this country and abroad who were neighbors of applicant during residence abroad.

3. REFERENCES. The name and addresses of individuals living in this country who were closely associated with applicant and who can verify applicant's addresses, employment, and activities in the foreign country.

4. ADDRESSES. The names, addresses, and occupations of nonrelatives with whom the applicant has resided in a foreign country.

5. RELATIVES. Determine the occupation and verify the full name of all relatives listed on the Personnel Security Questionnaire, and any other relatives residing in Communist-controlled countries or countries that are hostile to the United States. If a relative is employed by a foreign government, secure the details. Ascertain the degree and frequency of contact with these relatives.

6. CORRESPONDENCE. The names, addresses, and occupations of individuals (other than relatives covered in item 5 above) residing outside the U.S. with whom the applicant corresponds, including the nature of the correspondence.

7. ORGANIZATIONS. Determine the applicant's membership in all foreign organizations, except religious, including the date of membership and offices held. Develop the nature and purpose of the organization and the applicant's reason for joining, where appropriate.

CHAPTER III

SCREENING AND ANALYSIS OF PERSONNEL SECURITY CASES AND METHODS FOR DETERMINING ACCESS AUTHORIZATION ELIGIBILITY

1. SCREENING. Upon receipt of completed full field investigations, National Agency Checks and Inquiries, or National Agency Checks with Credit, the individual assigned the function of screening will check the investigative reports to assure that the items listed on the Personnel Security Questionnaire (DP-1), SF-85, SF-86, or other related forms have been covered.

   a. Full Field (background) Investigations.

      (1) Points of residence, employment, education, military service, etc., are checked to ascertain that they have in fact been adequately covered by the investigation.

      (2) All items of information of a derogatory nature (except minor traffic violations) are noted. Similarly, information which mitigates or negates the reported derogatory information is noted.

      (3) Those cases in which the investigation is complete and in which no derogatory information is reported are appropriately documented. If the individual assigned to this function has been delegated authority in writing to grant access authorization in this type of case the file shall be appropriately noted that access authorization is to be authorized. However, prior to the dispatch of notifications of the granting of access authorization there shall be a review of at least 10 percent of such cases by a senior security analyst for verification that the investigation is in fact complete and that derogatory information is not present. Such verification shall be documented by the signature of the reviewing official on the File Summary Sheet (DOE Form 5631.16).

      (4) A File Summary Sheet is completed and signed, the reports of investigation, DP-1, SF-86, or SF-85 and related documents are properly arranged in the file folder, and the case is forwarded to designated personnel for further processing of the case.

   b. National Agency Checks (NAC), National Agency Checks and Credit (NACC), National Agency Checks and Inquiries (NACI), and National Agency Checks and Inquiries and Credit (NACIC): It is determined that all items for scope of these checks as stated in 1a above are covered, and any derogatory information is noted.

2. ANALYSIS.

   a. Analysis of reports of investigation is designed to evaluate the reported information, favorable and unfavorable, in relation to the Criteria and Procedures for Determining Eligibility for Access to Classified

Matter and Significant Quantities of Special Nuclear Material, (10 CFR Part 710, hereafter referred to as "Criteria") and to determine whether the reported information raises a substantial doubt as to such eligibility. Frequently, the reported derogatory information standing alone would raise such a question but will be offset when considered with other reported mitigating information. Therefore, the analysis of personnel security cases shall not be performed as a mechanical or routine function, but rather as one of the most important aspects of the overall personnel security program.

b. If the investigation is complete in all respects and reported derogatory information is clearly outside the scope of the Criteria, the manager of the field office, or the individual who has been delegated this authority in writing, may grant access authorization:

(1) On the existing record.

(2) Or after additional investigation, psychiatric evaluation, or informal interview which extends or further clarifies the reported information.

(3) However, in cases where the reported information falls within one or more of the categories in the Criteria, manager of the operations office shall refer to the Director of Safeguards and Security (DP-34), a duplicate of the personnel security file together with a summary statement, and a recommendation as to the method to be employed in resolving the question(s) of the individual's eligibility for access authorization.

3. REFERRAL OF CASES FOR REVIEW AND ADVICE. Managers of the operations office are not precluded from referring any case to the Director of Safeguards and Security (DP-34) for review and advice as to whether the reported information falls within the Department's criteria. However, any case that is referred should reflect the opinion of the manager as to further action recommended.

4. ACTIONS AUTHORIZED BY THE OFFICE OF SAFEGUARDS AND SECURITY HEADQUARTERS (DP-34). The Director of Safeguards and Security, has been delegated the responsibility of reviewing all cases referred under 10 CFR Part 710.10, for determination of the method by which the question of eligibility for access authorization will be resolved. The Director of Safeguards and Security (DP-34) may:

a. Authorize the granting of access authorization on the existing records or after receipt of additional investigation.

b. Or determine that the question of eligibility cannot be resolved by additional investigation or interview, in which case the initiation of the Department's administrative review procedures (10 CFR Part 710.22 *et seq.*), is authorized.

5. INTERVIEWS. Since the DOE Criteria limits the use of the hearing procedure to cases in which questions of eligibility cannot be favorably resolved by interview, psychiatric evaluation, or additional investigation, the conduct of interviews is a most important function of a personnel security official.

   a. If it has been determined that an interview is necessary, the person assigned to conduct the interview will be fully qualified as an interviewer and shall be cognizant of all the questions or items of information to be explored. In other words, if a given case warrants an interview, the interviewer shall assure that it is properly conducted and that it will accomplish its purpose.

   b. A verbatim transcript or recording of interviews conducted in cases evaluated as containing substantially derogatory information is required. In cases containing non-substantially derogatory information, the interview may be transcribed, recorded, or summarized. If, however, the interview is conducted for the purpose of determining whether reported information is substantially or nonsubstantially derogatory in relation to the DOE criteria, a verbatim transcript or recording shall be made.

6. INTERROGATORIES. As an alternative to conducting an interview, a letter of interrogatory may be sent to the individual provided the information required is not of a serious nature (i.e., an unlisted relative), and/or the geographic location of the subject would make it extremely difficult to arrange for a personal interview.

7. ADDITIONAL INVESTIGATIONS. When an additional investigation is required to expand, resolve, or corroborate information, the request can be made directly to the local OPM or FBI Supervisory Investigator.

8. SPECIAL UPDATES. In those cases in which the investigation was completed by the OPM within the most recent 18 months, OPM shall conduct a "special update" full field investigation at a reduced rate of charge. Such requests should be transmitted to OPM using a DOE Form 5631.24 which is marked "special update" case.

9. ADMINISTRATIVE REVIEW PROCEDURES. The following subparagraphs briefly summarize the procedures to be followed when it has been determined by the Director of Safeguards and Security (DP-34), under 10 CFR Part 710, and an individual's eligibility for access authorization cannot be favorably resolved by interview, further investigation, or other means.

   a. The following explanation of the implementation of the DOE Administrative Review Procedures is furnished for guidance:

      (1) In those cases where the reported substantially derogatory information is not favorably resolved through an interview, psychiatric evaluation, or additional investigation, the Director

of Safeguards and Security (DP-34), shall authorize proceedings in accordance with 10 CFR Part 710.

(2) In cases where the individual currently holds DOE access authorization, the manager of operations office shall consider suspension of the individual's access authorization. If the manager determines that it is in the best interest of the national security to remove the individual from access to classified information or material, the manager shall direct the immediate suspension of access authorization.

(3) The notification letter shall be prepared and transmitted to the individual by the field office. Upon receipt of a written answer under oath or affirmation wherein the individual requests a hearing, a DOE attorney shall be assigned to act as Hearing Counsel. The Hearing Counsel shall review the response to the notification letter in relation to the information in the case, and in accordance with the specific arrangements for confrontation, shall request the Director of Safeguards and Security (DP-34), through the manager of the operations office, to produce the necessary witnesses and documents.

(4) If the local field office has not already done so, the Director of Safeguards and Security (DP-34) shall request the appropriate investigative agency to determine the willingness of the witnesses in question to appear before a Hearing Officer. If the witnesses are confidential informants within the meaning of Executive Order 10865, the investigative agency shall furnish a certification. If a witness, other than a confidential informant, is not willing to appear or is not available to testify, the investigative agency shall be requested to obtain the specific reasons for nonavailability. In those instances where the witness is not willing to appear, the investigative agency shall be requested to furnish advice as to whether the issuance of a subpoena by the DOE shall jeopardize investigative techniques or methods. Further, the investigative agency will be requested to undertake such additional investigation as necessary to develop other informants who may testify concerning the specific allegation controverted by the individual, when possible.

(5) Upon receipt of the supplemental reports from the investigative agency, the manager of the operations office may request:

(a) The issuance of a subpoena for those witnesses who are willing to appear before the Hearing Officer, or for those witnesses whose testimony will not jeopardize investigative techniques or methods. Subpoenas shall be issued by the Assistant Secretary for Defense Programs (DP-1).

(b) The Assistant Secretary for Defense Programs (DP-1) to make a determination pursuant to the procedures that a person furnishing adverse information which is controverted by the individual cannot appear to testify due to death, severe illness, or other cause believed to be good and sufficient.

(c) The Assistant Secretary for Defense Programs (DP-1) to make a determination pursuant to the procedures that classified physical evidence pertaining to adverse statements controverted by the individual may be received and used without affording the individual the opportunity to inspect such data.

(6) The manager of the operations office, or the Director of Safeguards and Security (DP-34), for Headquarters cases, may, with the concurrence of the Office of General Counsel, amend the notification letter whenever appropriate. The manager of the operations office shall keep the Hearing Counsel fully informed of the results of any supplemental investigation, and will forward as appropriate the subpoenas, the certifications, the determinations of exceptions to confrontation, or the amendments to the notification letter.

(7) The Hearing Counsel, thereafter, shall prepare the presentation of the case, contacting the individual, or his/her attorney, for the purpose of reaching mutual agreement upon arrangements for the hearing. When the Hearing Counsel has completed such arrangements, the manager shall appoint the Hearing Officer.

(8) The proceedings of the hearing shall be conducted by the Hearing Officer. The Hearing Counsel shall present evidence and conduct the direct examination and cross-examination of witnesses. The notification letter to the individual as well as the individual's response shall be introduced by the Hearing Counsel. No adverse information may be introduced by the Hearing Counsel unless such information or its substance has been made available to the individual, and no adverse information controverted by the applicant may be introduced by the Hearing Counsel, unless the individual has offered no objection to its presentation, or the individual is afforded an opportunity to cross-examine the person providing the information, or unless specific exceptions to confrontation have been authorized.

(9) The Hearing Officer shall make specific findings with respect to the allegations contained in the notification letter introduced during the hearing proceedings and shall predicate a recommendation on such findings.

(10) The findings and recommendation of the Hearing Officer, together with the record developed during the hearing proceedings, shall

be transmitted by the field office to the Assistant Secretary for Defense Programs through the Director of Safeguards and Security (DP-34). This shall be accompanied by the manager's advice as to the operational consequences of a denial or revocation of access authorization.

(11) In those cases where the Hearing Officer has recommended denial or revocation of access authorization, the Director of Safeguards and Security (DP-34), shall notify the individual, of his/her right to request a review of his case by the DOE Personnel Security Review Examiners. The individual shall be advised of the findings of the Hearing Officer. In those cases where the Hearing Officer has recommended favorably, the Assistant Secretary for Defense Programs may still refer the record to the DOE Personnel Security Review Examiners for advice. In such cases, the individual shall be notified of such referral.

(12) The DOE Personnel Security Review Examiners, based upon review of the record supplemented by the individual's brief, may recommend that the case be remanded, request additional investigation, or make findings and recommendation with respect to the specific allegations contained in the notification letter introduced during the hearing before the Hearing Officer. Each Review Examiner shall refer such findings and recommendations, together with the record, to the Assistant Secretary for Defense Programs.

(13) The final determination shall be made by the Assistant Secretary for Defense Programs, except in those cases where exceptions to the confrontation have been used and the Assistant Secretary for Defense Programs recommends adversely. In those cases the Secretary shall make the final determination.

(14) In the event the individual being considered under administrative review procedures no longer requires access authorization, the field office shall promptly notify Headquarters in writing. Action on the case shall be terminated unless the consolidated case has been forwarded to the Assistant Secretary for Defense Programs for a final determination.

10. PERSONS TREATED FOR MENTAL ILLNESS. To assist in determining whether reported information involving mental illness falls within the Criteria (10 CFR 710.11), the following guidance is provided:

a. When a DOE or contractor employee or consultant possessing DOE access authorization is hospitalized or otherwise treated for a mental illness which may cause a defect in judgment or reliability, the DOE supervisor or a responsible official or a DOE contractor shall report this information to the manager of the congnizant field office. Upon determination by the employer that the employee or consultant is able to perform his regular duties, the individual's access to classified information may be continued unless the manager of the field office determines that there is a significant defect in such individual's judgment or reliability with the meaning of 10 CFR Part 710.11(h) (in which case the procedures outlined in subparagraph 10c below shall be followed).

b. For the purpose of making a determination concerning the individual's judgment or reliability, the manager may accept previously rendered competent medical advice or records in possession of the DOE or DOE contractor. The manager may also, have a psychiatric examination conducted by a qualified physician designated by the DOE. In such a case the individual shall be requested to submit to an examination and to execute a consent form for such examination, Form DOE F 5631.10.

   (1) The psychiatrist shall submit a written report to the manager indicating his/her opinion as to whether the individual suffers from a mental illness or condition which causes a significant defect in the individual's judgment or reliability.

   (2) If the individual refuses to submit to an examination, the manager shall refer the case to the Director of Safeguards and Security (DP-34), Headquarters.

c. If the manager finds that there may be a significant defect in the reliability or judgment of the individual, he/she shall make a determination as to whether the individual's access authorization should be suspended pending the administrative review procedure. The access authorization of an individual shall not be suspended except by direction of the manager of the operations office.

d. If a psychiatric examination is conducted as described on page III-7, paragraph 10b, the psychiatrist who is to examine the individual on behalf of the DOE shall be notified that he or she may be called upon to testify as a witness in a hearing before a Hearing Officer, if such a hearing is held. Only physicians consenting to testify should be designated for examining purposes. The examining physician shall not be appointed a Hearing Officer or as a Personnel Security Review Examiner.

11. DISCLOSURE OF REPORTED INFORMATION. Following notification to an individual of his opportunity to request a hearing before a Hearing Officer, the contractor or prospective contractor may, upon inquiry, be informed of the status of the case but not of the information requiring its referral to a Hearing Officer.

12. TIME ELEMENT IN PROCESSING CASES. The following time schedule shall be observed:

a. Initial screening and notification of the granting of access authorization shall be accomplished within 7 working days of the receipt of completed investigations which have been evaluated as not containing derogatory information.

b. Within 30 working days of the receipt of a completed investigation, one of the following actions shall be taken:

(1) Grant access authorization.

(2) Request additional investigation.

(3) Clarify reported information by interview or letter of interrogatory.

(4) Refer the case to the Director of Safeguards and Security (DP-34), as containing substantially derogatory information.

c. The Director of Safeguards and Security (DP-34), in cases determined to require administrative review, shall authorize the initiation of a hearing before a Hearing Officer within 30 working days of receipt of a completed duplicate Personnel Security File.

d. The manager of the operations office shall have 30 days to prepare and deliver a notification letter, enumerating the charges against the individual and explaining the DOE administrative review process, to the individual in question.

e. Upon receipt of the individual's request for a hearing before a DOE Hearing Officer, the manager of the operations office shall arrange for the conduct of the hearing within 90 days.

f. The Hearing Officer shall prepare and submit a report to the manager of the operations office within 30 days of receiving a copy of the transcript of the hearing. That report shall include specific findings as to each allegation contained in the notification letter, and shall include a recommendation as to the disposition of the case.

g. In the event the case is referred to the Personnel Security Review Examiners, they shall complete and submit their reports within 45 days of receipt of the case for review.

CHAPTER IV

INTERIM ACCESS AUTHORIZATIONS AND WAIVERS OF PREAPPOINTMENT FULL FIELD INVESTIGATIONS

1. GENERAL. Only under the most exceptional circumstances and when such action is clearly consistent with the national interest will any individual be permitted to have access to classified matter or will a DOE employee be allowed to occupy a critical sensitive position prior to completion of the appropriate investigation. In all cases, "Interim Access Authorization" to either Restricted Data or National Security Information, or waivers of preappointment full field investigations shall be considered temporary measures, pending completion of investigation which must be in process. Interim access authorization to Restricted Data shall be approved by the Assistant Secretary for Defense Programs, and interim access to National Security Information, and waivers of preappointment full field investigations shall be approved by the Secretary. Requests for interim access authorization shall be made only in cases where access to Restricted Data requires the individual to have a "Q" access authorization or when access to National Security Information requires a "Top Secret" access authorization. Employees or access permit holders or individuals whose access requires "L" or "Secret" access authorizations shall not be processed for interim access authorizations.

2. INTERIM ACCESS AUTHORIZATION TO RESTRICTED DATA.

   a. Requests for "Interim Access Authorization" (DOE Form DP-366) will be submitted directly to the Director of Safeguards and Security (DP-34), and must be supported by a certification that:

      (1) Serious delay or interference to an operation or project essential to a DOE program may be experienced unless the named individual is granted access to Restricted Data prior to completion of the authorization procedures.

      (2) The services of a qualified person previously cleared or authorized access by DOE cannot be obtained.

   b. If a full field investigation has not been requested prior to the request for interim access to Restricted Data, this request, accompanied by the forms required for the level of access authorization requested (see Chapter II) must be made concurrently with the submission of the DP-366.

3. INTERIM ACCESS AUTHORIZATION TO NATIONAL SECURITY INFORMATION. A request for interim access authorization to National Security Information may be submitted for consideration when such access is required to meet a critical need prior to completion of the clearance process. The authority to approve interim access to National Security Information rests with the Secretary.

a. Interim access authorization to National Security Information may be requested when:

   (1) A review of past employment and results of reference checks indicate that the possibility of derogatory information being developed by a full field investigation is remote.

   (2) The need to have the individual commence work involving National Security Information is clearly urgent and in the national interest.

b. For Headquarters cases, the head of the major first tier organization, or his/her deputy, or for individuals employed at field offices, the manager of the operations office, or his/her deputy must certify to the above conditions. This authority may not be redelegated. If there is a reporting relationship to a line official at Headquarters, that official must also certify that the conditions are met.

c. The head of the major first tier organization, or his/her deputy, or for individuals employed at field offices, the manager of the operations office, or his/her deputy, shall prepare and forward a memorandum to the appropriate Headquarters line official, if any, for certification and submission to the Director of Personnel, Headquarters. All requests must be submitted to the Director of Personnel at least 20 working days prior to the proposed entrance on duty date for new DOE employees, or the proposed effective date of reassignment for current DOE employees. The Director of Personnel will arrange for appropriate reviews with the Office of Safeguards and Security, and the Assistant Secretary for Management and Administration, and for Secretarial action.

4. WAIVER OF PREAPPOINTMENT FULL FIELD INVESTIGATION. DOE shall process requests for waivers of preappointment full field investigations in accordance with the procedures established in Chapter 736 of the Federal Personnel Manual (FPM). Waiver of the preappointment investigation requirement on persons entering "sensitive" positions may only be made made "in case of emergency" provided that "the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency." This general restriction is applicable only to Critical-Sensitive positions as DOE will not process waivers for Noncritical-Sensitive positions. Waiver of the preappointment investigation requirement may not be made in Special-Sensitive positions. Guidelines for determining position sensitivity are contained in FPM Chapter 731, Subchapter 2, "Position Sensitivity."

a. Waiver of preappointment investigation may be requested for an individual selected for a Critical Sensitive position when:

   (1) A review of past employment and results of reference checks indicate that the possibility of derogatory information being developed by a full field investigation is remote.

(2) Meaningful work for the organization can be accomplished by the individual without access to classified information, or if the individual is already a DOE employee who has been granted a security clearance, such access may be continued.

(3) The need to have the individual commence work as soon as possible is clearly an emergency and in the national interest.

b. For Headquarters cases, the head of the major first tier organization, or his/her deputy, or for individuals employed at field offices, the manager of the operations office, or his/her deputy, must certify to the above conditions. This authority may not be redelegated. If there is reporting relationship to a line official at Headquarters, that official must also certify that the conditions are met.

c. The head of the major first tier organization, or his/her deputy, or for individuals employed at field offices, the Head of the Field Organization, or his/her deputy, will prepare and forward a memorandum to the appropriate Headquarters line official, if any, for certification and submission to the Director of Personnel. All requests must be submitted to the Director of Personnel at least 20 working days prior to the proposed entrance on duty date for new DOE employees, or the proposed effective date of reassignment for current DOE employees. The Director of Personnel will arrange for appropriate reviews with the Office of Safeguards and Security, the Assistant Secretary for Management and Administration, and for Secretarial action.

d. Waivers of preappointment National Agency Checks and Inquiries (NACI's) will not be processed.

5. STANDARDS AND PROCEDURES.

a. The Office of Safeguards and Security (DP-34) will assure that the following checks have been made, without disclosing substantially derogatory information, prior to certifying security approval of interim access authorizations or waivers of preappointment full field investigations:

(1) The Personnel Security Questionnaire (DP-1) or SF-86 signed by the individual has been reviewed.

(2) DOE files and DOE contractor files have been checked, including the results of preemployment inquiries.

(3) FBI file and fingerprint check have been requested.

(4) The Office of Personnel Management Security Investigations Index has been checked.

(5) A full field investigation has been requested.

(6) Records from the individual's most recent employer have been checked.

(7) For current or former Federal employees, the security files at the former agency have been checked.

(8) The individual has been interviewed regarding any derogatory information that has been developed.

b. Requests for central FBI file and fingerprint checks and full field investigations for these cases shall be initiated by forwarding:

(1) Five copies of the DP-1 or SF-86, fingerprint cards, and an Authority to Release Information form (DOE Form 5631.18) with a special letter requesting full field investigation. In addition a special marking indicating "Interim Access Authorization" is stamped on:

(a) All copies of the DP-1 or SF-86.

(b) The fingerprint cards.

(c) The request for investigation letter.

(d) The transmittal jacket or envelope.

(2) The special letter to the OPM or FBI, as appropriate, shall request that a central FBI file check be made and the results furnished to the DOE as expeditiously as possible.

CHAPTER V

DATA ON SPOUSES

1. GENERAL. To implement section 145a of the Atomic Energy Act of 1954, as amended and Executive Order 10450, which require an investigation and report on an individual's character, associations, and loyalty, it becomes necessary that the DOE receive information concerning spouses. In investigations of applicants, inquiries and record checks are made with respect to spouses and former spouses named in the Personnel Security Questionnaire (DP-1) or SF-86. However, such checks cannot be made in the cases of DOE and DOE contractor employees when marriage occurs after the grant of access authorization without the cooperation of the individual in furnishing biographical data on his or her spouse. DOE requires the execution of a Data Report on Spouse (DOE F 5631.34) by individuals who, after the grant of DOE access authorization, marry an individual who does not or has not possessed a DOE access authorization. A Data Report on Spouse is also required for any cleared individual or applicant for access authorization who is married to a foreign or a naturalized U.S. citizen.

2. PROCEDURES.

   a. Cleared Individuals Who Marry U.S. Citizens.

      Upon receipt of duplicate completed forms in the appropriate field office:

      (1) A local agency check shall be made with respect to the spouse.

      (2) The duplicate copy of DOE F 5631.34 shall be forwarded to the Director of Safeguards and Security (DP-34) for use in requesting appropriate central file checks.

   b. Individuals Whose Spouses Are Foreign Nationals or Naturalized U.S. Citizens.

      (1) Applicants for access authorization shall submit, in addition to a Personnel Security Questionnaire (Form DP-1), SF-85, or SF-86 two copies of DOE F 5631.34.

      (2) Upon marriage to a foreign national or naturalized U.S. citizen, individuals who have been granted access authorization shall submit to the field office having jurisdiction two copies of DOE F 5631.34.

      (3) A copy of DOE F 5631.34 shall be referred to the investigative agency with the PSQ's in applicant cases, and to the Director of Safeguards and Security (DP-34), if the individual has been granted access authorization.

(4) The Director of Safeguards and Security (DP-34) shall initiate such investigation on the spouse of an individual who has been granted access authorization as may be appropriate, and forward the reports of investigation to the manager of the field office concerned, and make any necessary name change on the Central Personnel Clearance Index (CPCI).

c. DOE Cleared Female Employees Who Marry Cleared Individuals. When a female DOE or DOE contractor employee marries an individual who possess or has possessed a DOE access authorization, or has a name change as a result of change in marital status, the necessary name change must be made on the CPCI.

d. DOE Cleared Female Employees Who Marry Individuals Without DOE Clearance. When a female DOE or DOE contractor employee marries an individual who does not hold a DOE clearance, she shall have her name changed on the CPCI only if she legally assumes her spouse's surname. If the woman's maiden name has been legally retained, the personnel security file should be noted and a DOE F 5631.34 completed if required; but her name as reflected on CPCI can remain the same.

3. ADDITIONAL REQUIREMENTS. In reviewing the Data Report on Spouse and investigative reports received concerning a spouse who is a foreign national or naturalized U.S. citizen, special consideration shall be given to the following:

a. How recently has the spouse entered the U.S.?

b. Are the interests of the country of which the spouse is (or was) a citizen, inimical to the interests of the U.S.?

c. Does the spouse have close relatives residing in countries whose interests are inimical to those of the U.S. (to be evaluated in relation to 10 CFR Part 710)?

d. In cases involving a spouse who is a foreign national, has the spouse declared his or her intention to become a U.S. citizen?

CHAPTER VI

ACCESS AUTHORIZATIONS FOR FOREIGN NATIONALS AND INDIVIDUALS POSSESSING DUAL CITIZENSHIP

1. REQUIREMENTS. Access authorization may be granted to a foreign national or dual citizen only where there is a clear showing that the applicant has unique or very unusual talents or skills not possessed to a comparable degree by an available United States citizen, and the position for which the individual is being considered is one that is essential to DOE's program. The decision to consider a foreign national or dual citizen for access authorization must be based on the assumption that such an individual is a calculated risk. A determination must be made as to whether it is possible to obtain sufficient investigation to base a decision regarding access eligibility. An interview with the foreign national or dual citizen shall be conducted and shall reflect detailed information which will aid in the conduct of the investigation and the evaluation of the individual's eligibility for DOE access authorization.

2. STANDARDS AND PROCEDURES FOR PROCESSING FOREIGN NATIONALS.

   a. Field offices.

      (1) Received and consider requests for access authorizations for aliens originated by DOE offices and contractors under their jurisdiction.

      (2) Evaluate the security risk arising from foreign national status, considering the following factors:

         (a) The nationality of the foreign national.

         (b) Whether sufficient security investigation can be obtained.

         (c) Length of stay in the United States.

         (d) Family legal and financial ties abroad.

         (e) Whether and in what manner the foreign national has evidenced an intention to become a U.S. citizen.

      (3) Transmit those requests which appear consistent with the requirements expressed above, together with all information and documents described on page VI-2, paragraph 2d, to the Director of Safeguards and Security (DP-34).

(4) Upon approval of the request(s) by the Director of Safeguards and Security (DP-34), process the request(s) in accordance with Chapter II, except that the determination to grant access authorization for foreign nationals shall be made by the managers of the operations offices and, in Headquarters, to the Director of Safeguards and Security (DP-34), without power of redelegation.

(5) Forward to the Director of Safeguards and Security (DP-34):

(a) Duplicate personnel security file in those cases containing derogatory information.

(b) A report reflecting the data set forth on page VI-3, paragraph 2g, when foreign nationals are employed on work requiring DOE access authorization.

(c) Supplemental reports of any significant change in the individual's citizenship or employment status.

b. Heads of Headquarters Divisions and Offices. Review requests for foreign national access authorizations referred to them, and transmit to the Director of Safeguards and Security (DP-34) only those requests in which they find that the individual in question will materially benefit a DOE program by contributing unique or unusual skills or talents not possessed to any comparable degree by an available U.S. citizen.

c. The Director of Safeguards and Security (DP-34).

(1) Evaluates the security risk arising from alien status, taking into consideration those factors set form on page VI-1, paragraph 2a(2).

(2) Jointly determines with the interested Headquarters official whether the potential contribution in the individual case outweighs the security risk arising from foreign national status, and returns the application to the field office concerned with appropriate instructions regarding further processing.

(3) Maintains liaison with other Federal agencies having responsibilities with respect to foreign nationals.

d. Information Required to Process Requests for Access Authorization for Foreign Nationals.

(1) Personnel Security Questionnaire (DOE Form DP-1) fingerprint card, Authority to Release Information, (DOE Form 5637.1) and Security Acknowledgement (DOE Form 5631.18).

(2) Statement concerning program for which foreign national was recruited and specific access to classified information to be afforded.

(3) Statement indicating title of position, location and documentation indicating compliance with requirements expressed on page VI-1, paragraph 2a(2).

(4) Verbatim transcript or detailed summary of interview reflecting information which will aid in the conduct of the investigation and the evaluation of the individual's eligibility for access authorization including detailed information on steps taken by the individual to become a citizen of the United States; previous civilian or military service with a foreign government; family or other relatives abroad; family legal and financial ties abroad; and whether any are employees of a foreign government. Also, the names of citizens of the U.S. who can furnish information as to the individual's background and activities prior to his/her entrance into the U.S.

e. Scope of Investigation. A full field investigation shall be required for all levels of access authorization for foreign nationals. In cases where the individual has resided in, or has relatives living in a country where the language is written in a non-Roman alphabet (i.e. Hebrew, Arabic, Chinese, Japanese, Russian, etc.), the individual should furnish the identifying information on former overseas addresses and on relatives written in the other alphabet.

f. Extension, Transfer or Reinstatement of Access Authorization. Access authorization for a foreign national may be extended, reinstated, or accepted for transfer with the concurrence of the Headquarters official having functional interest in the work to be done by this individual in accordance with procedures provided in Chapter VII.

g. Reporting:

(1) The reports forwarded to the Director of Safeguards and Security (DP-34), as required on page VI-2, paragraph 2a(5), shall reflect the following:

(a) Full name of the foreign national.

(b) Alien registration number.

(c) Type and date of access authorization.

(d) Citizenship.

(e) Status of application for U.S. citizenship.

(f) Employer.

(g) Description of duties and access required.

(2) Supplemental reports shall reflect any substantial change in any of the above. In the event the foreign national becomes a citizen, the date and number of the naturalization certificate and place of naturalization shall be reported.

3. DUAL CITIZENSHIP. Individuals who possess dual citizenship status (i.e., who are a citizen of the United States and a citizen of another country--for example, the United Kingdom or Israel) may be processed for a DOE access authorization provided they are advised prior to the initiation of the investigation that they shall be required to formally renounce their other country citizenship before a DOE access authorization will be granted. If the individual agrees to take action to formally renounce their other country citizenship, the investigation may be initiated with the appropriate investigative agency.

a. Prior to an individual being granted a DOE access authorization, they must provide a notarized statement in which they attest to the fact that their other country citizenship has been formally renounced and that the renouncement has been formally accepted by an official representative of that other country's government. Copies of any documents completed by the individual to formally renounce their other country citizenship should accompany the notarized statement, as well as any document generated by the other country government which acknowledges that the individual is no longer considered a citizen of that country.

b. If an individual possessing dual citizenship status declines to renounce other country citizenship, they must be processed for a DOE access authorization in accordance with the requirements on page VI-1, paragraphs 2 and 3.

CHAPTER VII

EXTENSIONS, TRANSFERS, TERMINATIONS AND REINSTATEMENTS OF ACCESS AUTHORIZATIONS

1. EXTENSIONS AND TRANSFERS.

a. Definitions.

(1) Extension of an access authorization is an authorization by a field office which permits an individual who possesses an active access authorization under the jurisdiction of another field office manager to have concurrent access to classified matter or significant quantities of special nuclear material under the jurisdiction of the extending office.

(2) Transfer of an access authorization is an acceptance by a field office of the active access authorization granted by another field office simultaneously with the termination of that access authorization by the latter.

b. Requests for extension or transfer of access authorizations received by field offices shall contain the full name of an individual and his date of birth, social security and DOE file number (if known), in order to establish positive identification.

c. Procedures. The following procedures shall govern the handling of requests for the extension or transfer of active access authorizations.

(1) The field office having custody of the individual's personnel security file shall inform the office extending the access authorization or accepting it for transfer of the following:

(a) The individual's date of birth.

(b) The individual's clearance status.

(c) The type of investigation upon which access authorization was granted.

(d) If reinvestigated, date and action taken.

(e) Whether or not the personnel security file contains unresolved substantially derogatory information.

(2) After positive identification has been established and on the basis of the information received, the individual's access authorization shall be extended or accepted for transfer unless the personnel security file contains unresolved substantially derogatory information.

(3) In case of transfer, when the personnel security file is received it shall be reviewed and noted to that effect before being sent to files.

(4) When supplemental investigation is deemed appropriate, requests for such investigation shall be submitted directly to the investigative agency.

(5) In cases involving the extension or transfer of an access authorization to a position certified as being "of a high degree of importance or sensitivity" and where the previous investigation was conducted by the Office of Personnel Management or other Federal agency, the request for the new investigation shall be forwarded to the FBI accompanied by new Personnel Security Questionnaire (PSQ), fingerprint record and one copy each of the previous investigative reports (see Chapter IV for detailed instructions). (Where such individuals transfer from the industrial program to DOE employment new PSQ's shall be obtained.)

(6) An access authorization shall not be accepted for extension or transfer in any case in which substantially derogatory information developed subsequent to the initial grant of access authorization has not been resolved. Such cases shall be referred to the Director of Safeguards and Security (DP-34), in accordance with Chapter IV.

d. Documentation of Extensions and Transfers. The office extending the access authorization and the office accepting the transfer of an access authorization shall notify the Central Personnel Clearance Index (CPCI) using instructions contained in the Central Personnel Clearance Index System Reference Manual.

e. Access Permit Program. "Q" and "L" access authorizations may be extended or transferred when appropriate to the Access Permit Program and reclassified as "Q(X)" or "L(X)" access authorizations. Similarly "Q(X)" and "L(X)" access authorizations may be extended or transferred when appropriate to DOE contractor operations and reclassified as "Q(N)" and "L" access authorizations.

f. Interim Access Authorizations. Interim access authorizations will not be extended or transferred.

g. In the event the office that originated the clearance terminates access authorization, the file shall be sent to the office to where the access authorization had been extended (see page VII-4, paragraph 2e).

2. TERMINATIONS.

a. Definition. Termination of access authorization is the discontinuance of an authorization for an individual to have access to classified matter or significant quantities of special nuclear material. (For the purposes of this part, terminations do not include suspensions or revocations.)

b. Field offices shall terminate access authorizations when:

(1) Employment by the Department of Energy is terminated.

(2) Access authorization is no longer required.

(3) An individual on a leave of absence or on extended leave, who will not require access for at least 90 days. This 90 day period may be adjusted at the discretion of the manager of the Operations office, or the Director of Safeguards and Security (DP-34).

(4) Access to classified matter or significant quantities of special nuclear material is no longer required by reason of termination of employment or transfer to a position not requiring such access. Exceptions may be authorized upon certification by the employer that the individual shall be reemployed or reassigned with access within 3 months and that DOE shall be kept informed of the individual's status.

(5) An individual goes on foreign travel, employment, education, or residence of more than 3 months duration not on official U.S. Government business.

c. Procedures. When access authorization is terminated, field offices shall:

(1) Obtain a Security Termination Statement (Form DP-5631.29) from the individual.

(2) Note in the individual's personnel security file that date and reason for termination.

(3) Make appropriate entry to the Central Personnel Clearance Index.

d. Termination Because of Foreign Travel. When access authorization is to be terminated as required on page VII-3, paragraph 2b(5), the individual shall, if practicable, be advised that his access authorization is being terminated and the reason therefore and shall also be informed that it may be reinstated when he resumes work requiring it. The reinstatement procedure may require new security forms and/or an updated investigation as noted on page VII-4, paragraph 3.

e. Transfer of Personnel Security Files of Terminated Cases. When a personnel security file of an individual whose access authorization has been terminated is transferred to another field office for retention, the office that is transferring the file shall enter the new file location on the Central Personnel Clearance Index.

f. Central Personnel Clearance Index (CPCI). The Office of Safeguards and Security, Headquarters, shall maintain a central record of individual terminations and location of files of individuals whose access authorizations have been terminated.

3. REINSTATEMENTS.

a. Definition. Reinstatement of access authorization permits an individual whose access authorization has been terminated to again have access to classified matter or significant quantities of special nuclear material.

b. Procedures.

(1) New Forms. An up-to-date Personnel Security Questionnaire (PSQ, DOE Form DP-1) shall be obtained if more than 6 months has elapsed since termination of access authorization and more than a year has elapsed since the date of the previous PSQ or any significant changes are known to have occurred since that date. Where PSQ's are not received, requests for reinstatements should contain the date of birth of the individual in order to establish positive identification. A new Security Acknowledgement (Form DP-15) shall be obtained in all cases.

(2) Personnel Security File. A review shall be made of the personnel security file of the individual to determine that the individual being reinstated is identical with the individual whose file is being reviewed and whether the previous investigation consisted of an National Agency Check or a full field investigation by the FBI, OPM or other Federal agency.

(3) Requests for Supplemental Investigation or National Agency Check for Reinstatement.

(a) Supplemental Investigation shall be requested prior to reinstatement when:

1 New and substantially derogatory information has been developed and has not been resolved subsequent to the initial grant of access authorization.

2 The reason for the previous termination was one affecting eligibility for access authorization.

3 In any "Q" type case more than 10 years has elapsed since the previous investigation and more than 5 years since the access authorization of the individual has been terminated.

(b) National Agency Checks may be requested, at the discretion of field offices in the reinstatement of any level of access authorization when none of the factors on page VII-4, paragraph 3b(3)(a) are present.

(c) Procedure for Supplemental Investigation for Reinstatement. In requesting supplemental investigation, four copies of new PSQ's stamped "Supplemental Investigation," fingerprint cards or other fingerprint record, and a Request for Investigation (Form DP-5631.23 or DP-5631.24) shall be forwarded to the appropriate investigative agency. Where the previous investigation was not made by the same investigative agency, one copy of each report of the previous investigation shall accompany the request and a copy of the previous PSQ.

(4) Positions "Of a High Degree of Importance or Sensitivity". Where the reinstatement involves the assignment of an individual to a position "of a high degree of importance or sensitivity" (see Chapter I) and the previous investigation was not conducted by the Federal Bureau of Investigation (FBI), a new PSQ together with one copy of each investigative report shall be forwarded to the FBI for investigation. Field Offices may authorize the reinstatement of access authorization prior to receipt of the new investigation by the FBI providing the circumstances listed on page VII-4, paragraph 3b(3)(a) do not apply.

(5) Reinvestigations. Where the reinstatement involves an individual falling within the scope of the reinvestigation program, the case shall concurrently be processed for reinvestigation (see Chapter VIII).

4. TRANSMITTAL OF PERSONNEL SECURITY FILES. Personnel security files being transferred by mail shall be sent via "First Class" mail except those classified Secret which shall be sent via registered mail. This applies to active or inactive files and the mailing of one or more investigative reports to the investigative agencies, DOE Headquarters, or other DOE field offices. A memorandum or other transmittal form shall be used to assure that a record of the location of personnel security files and reports is maintained. Files shall be transmitted in double envelopes, the inner envelope marked "Security Mail - To Be Opened Only By Security Personnel."

CHAPTER VIII

SELECTIVE REINVESTIGATION PROGRAM

1. GENERAL INFORMATION. The DOE Reinvestigations Program is designed to assure the continued eligibility for access authorization of individuals employed in classified programs of the Department of Energy. It applies to all individuals possessing DOE security clearance or access authorization except the following:

   a. DOE contractor construction personnel.

   b. Members of the Armed Services.

   c. Employees of agencies of the Department of Defense and their contractors.

   d. Employees of other Executive Branch departments or agencies and their contractors who hold DOE "Q" non-sensitive or "L" access authorization.

   e. Holders of access permits and their employees.

2. REEVALUATION. The eligibility of access authorization of individuals holding DOE access authorization shall be reevaluated each 5 years on the basis of either field reinvestigations, National Agency Check with Credit (NACC), file and fingerprint checks, or review of Personnel Security Questionnaires.

3. DETERMINING THE TYPE OF REINVESTIGATION TO BE CONDUCTED. The type and schedule of reinvestigation to be conducted shall be determined by the level of access authorization held by the individual.

   a. "Q" sensitive position that has also been designated to be a "Position of a High Degree of Importance or Sensitivity" (guidelines for making this determination are contained on page I-2, paragraph 3a(1)):

      (1) After first 5 years - Federal Bureau of Investigation (FBI) full field investigation.

      (2) After 10 and 15 years - National Agency Check with Credit (NACC).

      (3) After 20 years - FBI full field reinvestigation.

      (4) Each 5 years thereafter - NACC.

   b. "Q" and "Top Secret" (other than those described on page VIII-1, paragraph 3a):

      (1) After first 5 years - Office of Personnel Management (OPM) Background Investigation (BI).

      (2) After 10 and 15 years - NACC.

      (3) After 20 years - OPM Special Background Investigation (SBI).

(4) Each 5 years thereafter - NACC.

c. "L" and "Secret":

(1) After first 5 years - NACC.

(2) After 10 and 15 years - review of completed Personnel Security Questionnaire or SF-86, plus FBI file and fingerprint check.

(3) After 20 years - NACC.

(4) Each 5 years thereafter - review of completed PSQ or SF-86, plus FBI file and fingerprint check.

4. SCHEDULING REINVESTIGATIONS. The manager of the operations office shall establish a schedule for the submission of requests for and evaluation of reports of reinvestigation for cases under his or her jurisdiction.

5. EVALUATION PROCEDURES. The results of the reinvestigation shall be screened and analyzed following the procedures described in Chapter III. The results of the evaluation shall be entered onto the Central Personnel Clearance Index following the instructions contained in the Central Personnel Clearance Index System Reference Manual.

DOE Form DP-1
Part I

PRIVACY ACT STATEMENT

Collection of the information requested is authorized by the Atomic Energy Act of 1954, as amended, Chapter 12, Sections 141, 145(b), 161(b), and 161(i); and by Executive Orders 10450, 10865, and 12356.

Personal information on the form will be used to determine an individual's eligibility for DOE access authorization, security clearance or unescorted access to DOE security areas, or suitability for Federal employment. This form will become part of the individual's Personnel Security File (Department of Energy System of Records DOE-43, "Personnel Security Files").

The name of the individual, Social Security Number, and date of birth are used as identifying factors to establish and maintain records of DOE personnel clearance actions in DOE System of Records DOE-42, "The Personnel Security Clearance Index."

Some of the information on the form may also be used for statistical analysis in a health and mortality study related to radiation exposure as described in DOE System of Records DOE-72, "The Department of Energy Radiation Study Registry."

Disclosure of the information on this form is voluntary. However, if the information is not provided, the request for DOE access authorization, security clearance, or unescorted access to DOE security areas cannot be processed.

Routine Uses

Access to the completed form is permitted only to authorized Federal Government investigative agencies conducting the investigation for the DOE. In addition, the completed form may be released to other Federal agencies for the purpose of making security clearance determinations.

PART I – FRONT

DOE Form DP-1 (Part I)
(Rev. 8/83)
Exception to Standard Form 86
Approved by O.M.B.

U.S. DEPARTMENT OF ENERGY
Washington, D.C. 20545

Form Approved
O.M.B. 1910-0016

PERSONNEL SECURITY QUESTIONNAIRE

(Previous Editions are Obsolete)

- *INSTRUCTIONS—DOE Form DP-1 HAS TWO PARTS. ALL SECTIONS OF BOTH PARTS MUST BE COMPLETED. UNLESS BOTH PARTS ARE COMPLETELY AND PROPERLY EXECUTED, THE FORM WILL NOT BE ACCEPTED. Before any entries are made, familiarize yourself with all questions. Do not sign without first reading the instructions and certification at the end of the form. TYPE ALL ANSWERS. If more space is required, enter in item 17 on the back of this form or attach additional sheets and indicate the item numbers to which the answers apply. Questions which do not apply should be marked "None."*

1. NAME *(Last, First, Middle)*

4. DESCRIPTION

Male or Female	Height	Weight	Color Eyes	Color Hair

2. ALL OTHER NAMES *(Include maiden name, names by former marriages, and dates that names were used)*

5. SOCIAL SECURITY NO.

6. BIRTH DATE

Month	Day	Year

7. BIRTHPLACE *(City, County, State, and Country)*

3. PRESENT RESIDENCE *(Street and Number, City and State)* SINCE (Mo./Yr.)

8. Put an "X" in Appropriate Box(es): Single ☐ Married ☐ Widow(er) ☐ Divorced ☐
Dates and Places of marriages and if applicable, divorces

9. ALL OTHER RESIDENCES FOR PAST 15 YEARS FROM (Mo./Yr.) TO (Mo./Yr.)

10. CITIZENSHIP: U.S. ☐ Alien ☐ Dual ☐ Country other than U.S.

A. If U.S. Citizen, indicate whether:

(1) By Birth ☐	(3) By Naturalization ☐
(2) Derivative ☐	Alien Registration No.
Date	Petition No.
Certification No.	Date
Place	Certification No.
	Place

B. If alien, indicate:

(1) Alien Registration No.	(2) Present Citizenship
(3) Date of Entry	(4) Port of Entry

11. MILITARY SERVICE *(Past or Present)*

Serial Nos.	Branch	From (Yr.)	To (Yr.)

12. *EMPLOYMENT (List ALL employment dates including present employment and ALL dates and addresses when unemployed. If any employments required DOE security clearance or access authorization, indicate this fact after the name of the company or organization which requested the clearance. Give name or names under which employed if different from name now used.)*

Date From (Mo./Yr.) To (Mo./Yr.)	Name of Employer (Company or Organization)	Address (Where employed)	Type of Work	Supervisor's Name

13. FOREIGN COUNTRIES VISITED *(Exclusive of Military Service and U.S. Government Official Travel)*

Country	Purpose	Date Left USA	Date Returned USA

14. EDUCATION *(All Schools Above Elementary)*

Name of School	Address	From	To	Degree

15. RELATIVES *(Parents, stepparents, foster parents, spouse, divorced spouse or spouses, children, stepchildren, brothers, sisters, stepbrothers, stepsisters, half brothers, half sisters, father-in-law, and mother-in-law, living or dead. Name of spouse should include maiden name and any other names by previous marriage. If spouse is an alien, a naturalized U.S. citizen, or if you marry subsequent to the execution of this questionnaire, it will be necessary that data concerning your spouse be furnished on DOE Form DP-354.)*

Relation	Name in Full	Date of Birth	Address	Country of Birth	Present Citizenship

16. REFERENCES *(Name Three Persons, Not Relatives or Employers, Who Are Well Acquainted With You).*

Name in Full	Business and Home Address and Telephone Number	Years Known

CERTIFICATION

I have read all of the above questions. I certify that the information furnished in answer to these questions is correct and complete to the best of my knowledge and belief and I understand that it is of great importance in the consideration of my eligibility for security clearance or access authorization. I make this statement to the U.S. Department of Energy with the understanding that it will be used by the Department in carrying out its duty to protect the national security, and with knowledge that any false statement or omission of material fact may be sufficient cause for rejection of my application or dismissal after employment; further, that any false statement herein may be punished as a felony under Section 1001, Title 18, U.S. Code.

(Usual Signature of Person Filling Out Questionnaire) *(Sign Original Only)*

(Date and Place Where Signed)

TO BE FILLED OUT BY AGENCY OR FIRM EMPLOYING

BRIEF DESCRIPTION OF DUTIES *(Description should not Reveal Classified Information)*

(Signature and Title of Official Requesting Clearance or Access Authorization)

NAME OF AGENCY OR FIRM

ADDRESS

WILL PERSON HAVE ACCESS TO:

RESTRICTED DATA	Yes ☐	No ☐
NATIONAL SECURITY INFO	Yes ☐	No ☐
EXCLUSION AREA	Yes ☐	No ☐
SPECIAL NUCLEAR MAT.	Yes ☐	No ☐

PART I – BACK

PLEASE – Before Making any Entries on This Side: (1) Remove and Reverse Carbon Paper. (2) Reverse the Order of Copies (i.e., Copy One Front Side (Original) to be Copy One Reverse Side Also, etc.)

17. ADDITIONAL SPACE FOR FURNISHING INFORMATION IN ITEMS 1 TO 16. *(Indicate item numbers to which answers apply.)*

Item No.	

DOE Form DP-1
Part II

PRIVACY ACT STATEMENT

Collection of the information requested is authorized by the Atomic Energy Act of 1954, as amended, Chapter 12, Sections 141, 145(b), 161(b), and 161(i); and by Executive Orders 10450, 10865, and 12356.

Personal information on the form will be used to determine an individual's eligibility for DOE access authorization, security clearance or unescorted access to DOE security areas, or suitability for Federal employment. This form will become part of the individual's Personnel Security File (Department of Energy System of Records DOE-43, "Personnel Security Files").

The name of the individual, Social Security Number, and date of birth are used as identifying factors to establish and maintain records of DOE personnel clearance actions in DOE System of Records DOE-42, "The Personnel Security Clearance Index."

Some of the information on the form may also be used for statistical analysis in a health and mortality study related to radiation exposure as described in DOE System of Records DOE-72, "The Department of Energy Radiation Study Registry."

Disclosure of the information on this form is voluntary. However, if the information is not provided, the request for DOE access authorization, security clearance, or unescorted access to DOE security areas cannot be processed.

Routine Uses

Access to the completed form is permitted only to authorized Federal Government investigative agencies conducting the investigation for the DOE. In addition, the completed form may be released to other Federal agencies for the purpose of making security clearance determinations.

PART II – FRONT

DOE Form DP-1 (Part II)
(Rev. 8/83)
Exemption to Standard Form 86
Approved by O.M.B. 7

U.S. DEPARTMENT OF ENERGY
Washington, D.C. 20545

FORM APPROVED
O.M.B. 1910-0016

(Previous Editions are Obsolete)

PERSONNEL SECURITY QUESTIONNAIRE

1. NAME *(Last, First, Middle)*	2. SOCIAL SEC. NO.	3. NAME OF AGENCY OR FIRM EMPLOYING

INSTRUCTIONS – COMPLETE THIS FORM IN PRIVATE. ALL SECTIONS MUST BE COMPLETED. FORM WILL NOT BE ACCEPTED UNLESS COMPLETELY AND PROPERLY EXECUTED. The answers or statements on this form are privileged information between you and the Government. TYPE OR PRINT ALL ANSWERS. Write "None" when applicable. Enter in item 17 any additional information which may have a bearing on your security clearance. If more space is required, attach additional sheets and indicate the item numbers to which the answers apply. This form may be TYPED or PRINTED.

4. Are you now a member of the Communist Party, U.S.A., or any subdivision of the Communist Party, U.S.A.? YES ☐ NO ☐

5A. Are you now, or within the last 10 years have you been a member of any organization or group of persons including but not limited to the Communist Party, U.S.A., which, during the period of your membership or association you knew was advocating or teaching that the Government of the United States, or any State or any political subdivision thereof should be overthrown or overturned by force, violence, or any unlawful means? YES ☐ NO ☐

B. If your answer to A is "Yes", did you, during the period of such membership or association, have the specific intent to further the aims of such organization or group of persons to overthrow or overturn the Government of the United States or any State or any political subdivision thereof by force, violence, or unlawful means? YES ☐ NO ☐

6. If your answer to Questions 4. or 5a. above is "Yes", state below, under item No. 17, or on a separate sheet to be attached to and made a part of this questionnaire, the names of all such organizations and dates of membership. Give complete details of your activities therein and make any explanation you desire regarding your membership or activities.

NAME	ADDRESS	FROM	TO	OFFICE HELD

7. Are you now, or within the past 10 years have you been a member of any organizations (except labor unions and religious organizations) not covered by Questions 5. and 6. above? If your answer is "YES" provide details below, under item 17, or on a separate sheet of paper. YES ☐ NO ☐

NAME	ADDRESS	TYPE	FROM	TO	OFFICE HELD

8. Have you ever been arrested, charged or held by Federal, military, state, or other law enforcement or juvenile authorities? Include all instances in which you were arrested, charged, or held, even if the charges were dismissed. Include all court martial or nonjudicial punishment while in the military service. Do not include minor traffic violations for which a fine of $50 or less was imposed. If your answer is "Yes", complete all entries in item 9, below. YES ☐ NO ☐

9. ARRESTS (Complete A, B, C, and D for each case. Include all arrests and fines other than minor traffic violations even if the charges were dismissed.)

A. DATE	B. CHARGE	C. PLACE WHERE ARRESTED AND NAME OF LAW ENFORCEMENT AUTHORITY	D. ACTION TAKEN

A "YES" answer to any of the following questions (10, 11, 12, 13, 14, 15, or 16) MUST be explained. Use Item 17 on back, or additional sheets of paper, if necessary.

	YES	NO
10. Has your use of alcoholic beverages ever resulted in the loss of a job, arrest by police, or treatment for alcoholism?	☐	☐
11. A. Are you now, or have you been a user of any narcotic, hallucinogen, stimulant, depressant, or cannabis (to include marijuana and/or hashish), except as prescribed by a licensed physician?	☐	☐
B. Have you ever been treated for drug abuse?	☐	☐
12. Have you ever had a nervous breakdown or have you ever had medical treatment for a mental disorder?	☐	☐
13. Have you ever petitioned to be declared bankrupt or otherwise been the subject of bankruptcy proceedings, had a lien for non-payment of debts filed against your property, or been the subject of a civil judgment for failure to pay just debts?	☐	☐
14. Have you ever been released from the Armed Forces with other than an honorable discharge?	☐	☐
15. Have you ever been involuntarily terminated from a job?	☐	☐
16. A. To your knowledge, have you ever been investigated for, or granted a security clearance or access authorization by any department or agency of the Federal government?	☐	☐
B. To your knowledge, have you ever had a security clearance or access authorization denied, suspended, or revoked by any department or agency of the Federal government?	☐	☐

CERTIFICATION

I have read all of the above questions. I certify that the information furnished in answer to these questions is correct and complete to the best of my knowledge and belief and I understand that it is of great importance in the consideration of my eligibility for security clearance or access authorization. I make this statement to the U.S. Department of Energy with the understanding that it will be used by the Department in carrying out its duty to protect the national security, and with the knowledge that any false statement or omission of material fact may be sufficient cause for rejection of my application or dismissal after employment; further, that any false statement herein may be punished as a felony under Section 1001, Title 18, U.S. Code.

(Usual signature of person filling out questionnaire) *(Sign original only)* *(Date and place where signed)*

INSTRUCTIONS TO APPLICANT UPON COMPLETION OF ABOVE: Now that the form is signed, place it in the pre-addressed envelope furnished, sign across the envelope flap on the line provided, and affix the date of signature. Deliver the sealed envelope to you employer immediately or mail direct to the addressee.

PART II – BACK

PLEASE – Before Making any Entries on This Side: (1) Remove and Reverse Carbon Paper. (2) Reverse the Order of Copies (i.e., Copy One Front Side (Original) to be Copy One Reverse Side Also, etc.)

17. ADDITIONAL SPACE FOR FURNISHING INFORMATION IN ITEMS 1 TO 16. *(Indicate item numbers to which answers apply.)*

Item No.	

Form DP-1 (Part II) Back

PART 710—CRITERIA AND PROCEDURES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED MATTER OR SIGNIFICANT QUANTITIES OF SPECIAL NUCLEAR MATERIAL

GENERAL PROVISIONS

Sec.
710.1 Purpose.
710.2 Scope.
710.3 Reference.
710.4 Policy.
710.5 Definitions.

CRITERIA FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED MATTER OR SIGNIFICANT QUANTITIES OF SPECIAL NUCLEAR MATERIAL

Sec.
710.10 Application of the criteria.
710.11 Criteria.

PROCEDURES

710.20 Purpose of the procedures.
710.21 Suspension of access authorization.
710.22 Notice to individual.
710.23 Additional information.
710.24 Failure of individual to request a hearing.
710.25 Selection of DOE Hearing Counsel.
710.26 Appointment of Hearing Officers.
710.27 Conduct of proceedings.
710.28 Recommendation of the Hearing Officer.
710.29 New evidence.
710.30 Actions on the recommendations.
710.31 Recommendation of the DOE Personnel Security Review Examiners.
710.32 Action by the Assistant Secretary for Defense Programs.
710.33 Action by the Secretary.
710.34 Reconsideration of cases.

MISCELLANEOUS

710.35 Terminations.
710.36 Attorney representation.
710.37 Certifications.
710.38 Washington Area cases.

APPENDIX—SELECTED PROVISIONS OF THE ATOMIC ENERGY ACT OF 1954, AS AMENDED, SEC. 141 (42 U.S.C. 2161), SEC. 145 (42 U.S.C. 2165), SEC. 161 (42 U.S.C. 2201)

AUTHORITY: Sec. 145, 68 Stat. 942, as amended (42 U.S.C. 2165); sec. 161, 68 Stat. 948, as amended (42 U.S.C. 2201), E.O. 10450, 3 CFR 1949-1953 comp., p. 936, as amended; E.O. 10865, 3 CFR 1959-1963 comp., p. 398, as amended, 3 CFR, Chap. IV; sec. 104(c), 88 Stat. 1237 (42 U.S.C. 5814); sec. 105(a), 88 Stat. 1238 (42 U.S.C. 5815).

SOURCE: 42 FR 52382, Sept. 30, 1977, unless otherwise noted.

NOMENCLATURE CHANGES: 46 FR 18170, Mar. 23, 1981.

GENERAL PROVISIONS

§ 710.1 Purpose.

(a) This part establishes the criteria, procedures and methods for resolving questions concerning the eligibility of individuals who are employed by or applicants for employment with DOE contractors, agents, and access permittees of the DOE, individuals who are DOE employees or applicants for DOE employment, and other persons designated by the Secretary of the DOE, for access to Restricted Data or significant quantities of special nuclear material; pursuant to the Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974 or for access to national security information.

(b) This part is published to implement Executive Orders 10865, 25 FR 1583 (February 24, 1960) and 10450, 18 FR 2489 (April 27, 1954), both as amended.

§ 710.2 Scope.

The criteria and procedures outlined in this part shall be used in those cases in which there are questions of eligibility for DOE access authorization involving:

(a) Those employees (including consultants) of, and those applicants for employment with, contractors and agents of the DOE.

(b) Access permittees of the DOE and there employees (including consultants) and applicants for employment;

(c) Employees (including consultants) of, and applicants for employment with, the DOE; and

(d) Those other persons designated by the Administrator of the DOE.

§ 710.3 Reference.

The pertinent sections of the Atomic Energy Act of 1954, as amended, which remain in effect are set forth in Appendix A.

§ 710.4 Policy.

(a) It is the policy of DOE to carry out its responsibility for the security of the energy research and development programs in a manner consistent with traditional American concepts of justice. To this end, the Secretary has established criteria for determining eligibility for access authorization and will afford those individuals described in § 710.2 the opportunity for administrative review of questions concerning their eligibility for access authorization.

(b) In instances where the individual has been convicted of a felony crime, and is currently serving court ordered probation or parole, the DOE may withhold processing applications for security clearance or access authorization until such time as the individual completes serving the probation parole.

[48 FR 46500, Oct. 13, 1983]

§ 710.5 Definitions.

As used in this part:

(a) "Access authorization" means an administrative determination that an individual (including a consultant) who is employed by, or is an applicant for employment with DOE contractors, agents, and access permittees of DOE is eligible for access to Restricted Data or national security information or is eligible for access to, or control over, significant quantities of special nuclear material; and an individual (including a consultant) who is a DOE employee or applicant for DOE employment or otherwise designated by the Secretary of DOE is eligible for security clearance.

(b) For the purposes of this regulation, "significant quantities of special nuclear material" means unclassified special nuclear material, not subject to a Nuclear Regulatory Commission (NRC) license, in one facility or one shipment in the following quantities:

(1) Uranium 235 (contained in uranium enriched 20 percent or more in the Uranium 235 isotope) alone, or in combination with Plutonium and/or Uranium 233 when (multiplying the Plutonium and/or Uranium 233 content by 2½) the total is 1,000 grams or more.

(2) Plutonium and/or Uranium 233 when the Plutonium and/or Uranium 233 content is 400 grams or more.

(3) Special nuclear material in lesser quantities but which is located in the same area or shipment with other special nuclear material with which it could be selectively combined to produce the equivalent quantities in paragraph (b)(1) or (2) of this section.

(c) "DOE Personnel Security Review Examination" means a review process as described in § 710.31, in which the designated DOE Personnel Security Review Examiners individually and independently review questions concerning the eligibility or continued eligibility of those individuals described in § 710.2, and offer findings and recommendations to the DOE Assistant Secretary for Defense Programs.

(d) "DOE Personnel Security Review Examiners" are persons appointed by the DOE Assistant Secretary for Defense Programs who are designated to review questions concerning the eligibility or continued eligibility of those individuals described in § 710.2. Examiners shall be U.S. citizens and have a DOE "Q" clearance and shall not otherwise be in the employ of the DOE.

(e) "Hearing Counsel" means a DOE attorney assigned to prepare and conduct hearings as provided in §§ 710.26 and 710.27.

(f) "Manager of Operations" means the Manager of a DOE Operations Office, the Manager of Pittsburgh Naval Reactors Office, the Manager of Schenectady Naval Reactors Office (and at Headquarters, the Director, Office of Safeguards and Security—see § 710.38).

(g) "Hearing Officer" is an individual appointed by the Manager of Operations who, upon considering the evidence at a hearing, makes specific findings as to the truth of the derogatory information, and determines whether to recommend to the Manager of Operations the granting, denial, or revocation of an individual's access authorization. Hearing Officers shall be U.S. citizens and have a DOE "Q" clearance.

(h) "Secretary" means the head of the Department of Energy as provided by section 201 of the Department of Energy Organization Act.

(i) Throughout this part the use of the male gender shall include the female gender.

[46 FR 18170, Mar. 23, 1981 and 48 FR 46500, Oct. 13, 1983]

CRITERIA FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED MATTER OR SIGNIFICANT QUANTITIES OF SPECIAL NUCLEAR MATERIAL

§ 710.10 Application of the criteria.

(a) The decision as to access authorization is a comprehensive, commonsense judgment, made after consideration of all the relevant information, favorable or unfavorable, as to whether the granting of access authorization would endanger the common defense and security and would be clearly consistent with the national interest.

(b) To assist in making these determinations, on the basis of all the information in a particular case, there are set forth in this part a number of specific types of derogatory information. These criteria are not exhaustive but contain the principal types of derogatory information which create a question as to the individual's eligibility for access authorization. While there must necessarily be adherence to such criteria, DOE is not limited thereto, nor precluded from exercising its judgment that information or facts in a case under its cognizance are derogatory although at variance with, or outside the scope of, the stated categories. These criteria are subject to continuing review and may be revised from time to time as experience and circumstances may make desirable.

(c) When the reports of investigation of an individual contain information reasonably tending to establish the truth of one or more of the items in the criteria, such information shall be regarded as substantially derogatory and create a question as to the individual's eligibility for access authorization. The Manager of Operations may authorize an interview with the individual, or other investigation as deemed appropriate, and on the basis of such interview and/or investigation, may authorize the granting of access authorization. If the question as to the individual's eligibility is not resolved through interview, additional investigation, or when applicable, through a psychiatric evaluation, the Manager of Operations will forward the individual's case to the Director, Office of Safeguards and Security, DOE. The Director, Office of Safeguards and Security, DOE, may authorize: (1) The granting of access authorization, (2) such other investigation as the Director deems appropriate, or (3) the institution of the procedures set forth in § 710.20 et seq. The Director, Office of Safeguards and Security, must authorize one of these options within 30 days from the receipt of the case from the Manager of Operations, unless an extension is made by the Deputy Assistant Secretary for Security Affairs.

(d) In resolving a question concerning the eligibility or continued eligibility of an individual for access authorization, the DOE Hearing Officer shall consider the extent of activities, the period in which such activities occurred, the length of time which has since elapsed, and the attitudes and convictions of the individual in determining whether the recommendation will be adverse or favorable.

[40 FR 36302, Aug. 20, 1975, as amended at 47 FR 30718, July 15, 1982; 48 FR 46500, Oct. 13, 1983]

§ 710.11 Criteria.

Derogatory information included, but not limited to, those cases in which the individual has:

(a) Committed, prepared or attempted to commit, or aided, abetted or conspired with another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(b) Knowingly established or continued a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, espionage agent, or representative of a foreign nation whose interests are inimical to the interests of the United States, or with any person advocating the use of force or violence to overthrow the Government of the United States by unconstitutional means.

(c) Knowingly held membership in or had a knowing affiliation with, or has taken action which evidences a sympathetic association with the intent of furthering the aims of, or adherence to, and active participation in any foreign or domestic organization, association, movement, group, or combination of persons which advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or Laws of the United States or any state or subdivision thereof by unlawful means.

(d) Publicly or privately advocates, or participates in the activities of a group or organization, which has as its goal, revolution by force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means with the knowledge that it will further those goals.

(e) Parent(s), brother(s), sister(s), spouse, or offspring residing in a nation whose interests may be inimical to the interests of the United States, or in satellites or occupied areas thereof (to be evaluated in the light of the risk that pressure applied through such relatives could force the individual to act contrary to national security).

(f) Has deliberately misrepresented, falsified or omitted significant information from a Personnel Security Questionnaire, a personnel qualifications statement, or a personnel security interview.

(g) Has failed to protect classified information, or safeguard special nuclear material; or has willfully violated or disregarded security or safeguards regulations to a degree which would endanger the common defense and security or has intentionally disclosed classified information to a person unauthorized to receive such information.

(h) Has an illness or mental condition of a nature which in the opinion of competent medical authority causes, or may cause, significant defect in the judgment or reliability of the individual, or has refused to be examined by a psychiatrist.

(i) Has refused to testify before a Congressional Committee, Federal or state court, or Federal administrative body, regarding charges relevant to eligibility for DOE access authorization.

(j) Is a user of alcohol habitually to excess, or has been such without adequate evidence of rehabilitation or reformation.

(k) Has used, trafficked in, sold, transferred or possessed a drug or other substance listed in the schedule of Controlled Substances established pursuant to section 202 of the Controlled Substances Act of 1970 (such as amphetamines, barbiturates, narcotics, etc.) except as prescribed or administered by a physician licensed to dispense drugs in the practice of medicine, without adequate evidence of rehabilitation or reformation.

(l) Has engaged in any unusual conduct or is subject to any circumstances which tend to show that the individual is not honest, reliable, or trustworthy, and there is no adequate evidence of rehabilitation or reformation; or which furnishes reason to believe that the individual may be subject to coercion, influence, or pressure which may cause the individual to act contrary to the best interests of the national security. Such conduct or circumstances include but are not limited to sexual activity, demonstrated financial irresponsibility or notoriously disgraceful conduct.

[47 FR 30718, July 15, 1982]

PROCEDURES

§ 710.20 Purpose of the procedures.

These procedures establish methods for the conduct of hearings and administrative review of questions concerning an individual's eligibility for access authorization when it is determined that such questions cannot be favorably resolved by interview or other investigation.

[42 FR 52382, Sept. 30, 1977, as amended at 46 FR 18170, Mar. 23, 1981]

§ 710.21 Suspension of access authorization.

In those cases where information is received which raises a question concerning the continued eligibility of an individual for DOE access authorization, the Manager of Operations shall determine whether the individual's access authorization should be suspended pending the final determination resulting from the operations of the procedures provided in this part. In making the determination, the Manager of Operations shall consider such factors as the seriousness of the derogatory information developed, the possible access of the individual to classified information or significant quantities of special nuclear material, and the individual's opportunity by reason of the individual's position to commit acts adversely affecting the national security. The access authorization of an individual shall not be suspended except by direction of the Manager of Operations. Following the decision to suspend the individual's access authorization, the Manager of Operations shall immediately notify the Assistant Secretary for Defense

Programs through the Director, Office of Safeguards and Security. In addition, the Manager, within 10 days of the date of suspension shall submit a request for authority to conduct a hearing to the Director, Office of Safeguards and Security. This request should also contain an explanation of the basis for the suspension.

[48 FR 46501, Oct. 13, 1983]

§ 710.22 Notice to individual.

When the Director, Office of Safeguards and Security, has directed the institution of these administrative review procedures with respect to an individual's questioned eligibility for access authorization (as per § 710.10(c)), the Manager of Operations shall prepare a notification letter, approved by the local Office of Chief Counsel, for delivery to the individual within 30 days of the receipt of such directive from the Office of Safeguards and Security, unless an extension has been authorized by the Director, Office of Safeguards and Security. Where practicable, such letter shall be presented to the individual in person. The letter shall state:

(a) That reliable information in possession of DOE has created a substantial doubt concerning the individual's eligibility for access authorization;

(b) The information which creates a substantial doubt regarding the individual's eligibility for access authorization shall be as comprehensive and detailed as the national security permits;

(c) That in the event the individual desires a hearing the individual must, within twenty days of the date of receipt of the notification letter, indicate in writing to the Manager of Operations from whom the letter was received that the individual wishes a hearing before a Hearing Officer.

(d) That within twenty days of the date of receipt of the notification letter, the individual shall file with the Manager from whom he received such letter his written answer under oath or affirmation to each item of reported information which raises the question of the individual's eligibility for access authorization;

(e) That, if the individual so requests, a hearing will be scheduled before a Hearing Officer, with due regard for the convenience and necessity of the parties or their representatives, for the purpose of affording the individual an opportunity of supporting his eligibility for access authorization.

(f) That, if the individual requests a hearing, the individual will be notified in writing of the Hearing Officer's identity when the Hearing Officer is appointed by the Manager of Operations.

(g) That the individual will have the right to appear personally before a Hearing Officer, and present evidence in his own behalf, through witnesses, or by documents, or both, and subject to the limitations set forth in § 710.27(f), be present during the entire hearing and be accompanied, represented and advised by counsel of his own choosing;

(h) That the individual's failure to file a written request for a hearing before a Hearing Officer, in accordance with paragraphs (c) and (d) of this section, will be considered as a relinquishment by him of the opportunity of availing himself of the hearing and review procedure provided in this part, and that in such event a recommendation as to the final action to be taken will be made by the Manager of Operations and submitted to the Assistant Secretary for Defense Programs for decision on the basis of the information in the case without reference to a Hearing Officer;

(i) The individual's access authorization status until further notice;

(j) The name of the designated DOE official to contact for any further information desired.

[42 FR 52382, Sept. 30, 1977, as amended at 46 FR 18170, Mar. 23, 1981; 48 FR 46501, Oct. 13, 1983]

§ 710.23 Additional information.

A copy of this part shall be given to the individual with the notification letter.

§ 710.24 Failure of individual to request a hearing.

(a) In the event the individual fails, within the prescribed time, to file a written request for a hearing before a Hearing Officer, pursuant to § 710.22, a recommendation as to the final action to be taken shall be made by the Manager of Operations to the Assistant Secretary for Defense Programs on the basis of the information in the case;

(b) The Manager of Operations may for good cause shown, at the request of the individual, extend the time for filing a written request for a hearing or time for filing a written answer to the matters contained in the notification letter.

§ 710.25 Selection of DOE Hearing Counsel.

(a) Upon receipt from the individual of a written answer to the notification letter, signifying the individual's desire to appear before a Hearing Officer and answering under oath or affirmation the allegations contained in the notification letter, an DOE attorney shall forthwith be assigned by the Manager of Operations to act as Hearing Counsel;

(b) Hearing Counsel shall, prior to the scheduling of the hearings, review the information in the case and shall request the presence of witnesses and the production of physical evidence in accordance with the provisions of paragraphs (m), (n), (o), and (p) of § 710.27. When the presence of a witness is deemed by the Hearing Counsel to be necessary or desirable to a proper determination of the issues before the Hearing Officer, the Manager of Operations shall make arrangements by subpoena or otherwise for such witnesses to appear, be confronted by the individual, and be subject to examination and cross-examination.

(c) Hearing Counsel is authorized to consult directly with the individual if he is not represented by counsel, or if so represented with counsel or representative, for purposes of reaching mutual agreement upon arrangements for expeditious hearing of the case. Such arrangements may include clarification of issues and stipulations with respect to testimony and contents of documents and other physical evidence. Such stipulations when entered into shall be binding upon the individual and the Secretary for the purposes of this part. Prior to such consultation the Hearing Counsel shall advise the individual of his right to counsel or other representation and of the possibility that any statements made by the individual to the Hearing Counsel may be used in subsequent proceedings;

(d) The individual is responsible for producing witnesses in his own behalf or presenting other proof before the board to support the individual's answer and defense to the allegations contained in the notification letter. When requested, however, Hearing Counsel shall assist the individual to the extent practicable and necessary. In the Hearing Counsel's sound discretion he may request the Manager of Operations to arrange for the issuance of subpoenas for witnesses to attend the hearing in the individual's behalf, or for the production of specific documents or other physical evidence, provided a showing of the necessity for such assistance has been made.

[42 FR 52382, Sept. 30, 1977, as amended at 46 FR 18171, Mar. 23, 1981]

§ 710.26 Appointment of Hearing Officers.

(a) Upon notification from the Hearing Counsel that arrangements for an expeditious hearing have been completed, the Manager of Operations shall appoint a Hearing Officer.

(b) No person shall serve as a Hearing Officer who has prejudged the case to be heard; who possesses information that would impair his ability to render impartial recommendations or advice; or who for bias or prejudice generated for any reason would be unable to render fair and impartial recommendations or advice.

(c) Immediately upon the appointment of a Hearing Officer, the Manager of Operations will notify the individual of the identity of the Hearing Officer and of the individual's right to challenge the Hearing Officer for cause. Such challenge, accompanied by the reasons therefor, must be submitted to the Manager of Operations within seventy-two hours of the receipt of the notice of the identity of the Hearing Officer.

(d) In the event the individual challenges the Hearing Officer, the Manager of Operations will rule on the challenge. Where the challenge of the individual is sustained, the Manager of Operations shall appoint a new Hearing Officer and notify the individual. The individual shall have the right to challenge the new Hearing Officer for cause and such challenge shall be dealt with in the same manner as an original challenge. The Manager of Operations shall also notify the individual of the rejection of any challenge. The Hearing Officer shall convene a hearing as soon as is reasonably practicable.

(e) The Manager of Operations shall notify the individual in writing, at least one week in advance of the date, hour, and place the hearing will convene. In the event the individual fails to appear at the time and place specified, a recommendation as to the final action to be taken shall be made by the Manager of Operations to the Assistant Secretary for Defense Programs on the basis of the record in the case. At the request of the individual, however, the Manager of Operations may permit a hearing at a newly scheduled date, hour, and place for good cause shown.

[46 FR 18171, Mar. 23, 1981]

§ 710.27 Conduct of proceedings.

(a) The proceedings shall be conducted by the Hearing Officer in an orderly, impartial, and decorous manner with every effort made to protect the interest of the government and of the individual in determining the truth of the allegations. Hearings shall commence within 90 days from the date the individual's request for hearing is received. This period can only be extended with the approval of the Director, Office of Safeguards and Security, Headquarters, who will consider the effect of such extension on the interests of both the government and the individual. In performing duties, the Hearing Officer shall always bear in mind and make clear to all concerned that the proceeding is an administrative hearing and not a trial.

(b) The proceedings shall be open only to duly authorized representatives of the staff of DOE, the individual, counsel, and such persons as may be officially authorized by the Hearing Officer. Witnesses shall not testify in the presence of other witnesses;

(c)(1) Hearing Counsel shall examine and cross-examine witnesses and otherwise assist the Hearing Officer in such a manner as to bring out a full and true disclosure of all facts, both favorable and unfavorable, having a bearing on the issues before the Hearing Officer. In performing his duties, he shall avoid the attitude of a prosecutor and shall always bear in mind that the proceeding is an administrative hearing and not a trial;

(2) Hearing Counsel shall express no opinion to the Hearing Officer concerning the merits of the case. Hearing Counsel shall advise the individual of the individual's rights under these procedures when the individual is not represented by counsel of the individual's own choosing.

(d) The Hearing Officer may ask the individual, DOE representatives, and other witnesses any supplemental questions which the Hearing Officer deems appropriate to assure the fullest possible disclosure of relevant and material facts. The proponent of a witness shall conduct the direct examination of that witness;

(e) During the course of the hearing the Hearing Officer shall rule on all questions presented to the Hearing Officer for the Hearing Officer's determination.

(f) In the event it appears in the course of the hearing that Restricted Data or national security information may be disclosed, it shall be the duty of the Hearing Officer to assure that disclosure is not made to persons who are not authorized to receive it.

(g) The Hearing Officer shall admit in evidence any matters either oral or written which are material, relevant and competent in determining the issues involved, including the testimony of responsible persons concerning the integrity of the individual. The utmost latitude shall be permitted with respect to relevancy, materiality, and competency. Every reasonable effort shall be made to obtain the best evidence available. Hearsay evidence may for good cause shown be admitted without regard to technical rules of admissibility and accorded such weight as the circumstances warrant;

(h) Testimony of the individual and witness shall be given under oath or affirmation, and the individual and witnesses shall be subject to cross-examination. Attention of the individual and the witness shall be invited to 18 U.S.C. 1001 and 18 U.S.C. 1621;

(i) The individual shall be afforded the opportunity of testifying in his own behalf;

(j) The Hearing Officer shall endeavor to obtain all the facts that are reasonably available in order to arrive at recommendations. If, prior to or during the proceedings, in the opinion of the Hearing Officer the allegations in the notification letter are not sufficient to cover all matters into which inquiry should be directed, the Hearing Officer shall recommend to the Manager of Operations concerned that, in order to give more adequate notice to the individual, the notification letter should be amended. Any amendment shall be made with the concurrence of Counsel. If, in the opinion of the Hearing Officer, the circumstances of such amendment may involve undue hardships to the individual because of limited time to answer the new allegations in the notification letter, an appropriate adjournment shall be granted upon the request of the individual.

(k) Unless permitted by paragraphs (l), (m), (n), (o), and (p) of this section, the record may contain no information adverse to the individual on any controverted issue unless (1) the information or its substance has been made available to the individual and he offers no objection to its presentation; or (2) the information or its substance is made available to him and the individual is afforded an opportunity to cross-examine the person providing the information. Information whose admission is not prohibited by this paragraph, or by any other provision of this part, may be received and made a part of the record and may be considered by the Hearing Officer or officials charged with making determinations under this part;

(l) A written or oral statement of a person relating to the characterization in the notification letter of any organization or person other than the individual may be received and considered by the Hearing Officer without affording the individual an opportunity to cross-examine the person making the statement on matters relating to the characterization of such organization, or person, provided the individual is given notice that it has been received and may be considered by the Hearing Officer, and is informed of its contents provided such is not prohibited by § 710.27(f);

(m) The individual shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the individual relating to a controverted issue except that any such statement may be received and considered by the Hearing Officer without affording such opportunity in either of the following circumstances;

(1) The head of the department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of the informant's identity would be substantially harmful to the national interest;

(2) The Secretary or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the Secretary or such special designee has determined that failure of the Hearing Officer to receive and consider such statement would, in view of the access to Restricted Data, national security information, or significant quantities of special nuclear material sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (i) due to death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the individual, or (ii) due to some other cause determined by the Secretary to be good and sufficient;

(n) Whenever procedures under paragraph (m) (1) or (2) of this section are used (1) the individual shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, and (2) appropriate consideration shall be accorded to the fact that the individual did not have an opportunity to cross-examine such person or persons;

(o) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to DOE by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary to safeguard Restricted Data, national security information or significant quantities of special nuclear material.

(p) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the individual, may be received and considered provided that:

(1) The Secretary or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material;

(2) The Secretary or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the access to Restricted Data, national security information or significant quantities of special nuclear material sought, be substantially harmful to the national security; and

(3) To the extent that national security permits, a summary or description of such physical evidence shall be made available to the individual. In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency shall be considered.

(q) The Hearing Officer may request the Manager of Operations to arrange for additional investigation on any points which are material to the deliberations of the Hearing Officer and which the Hearing Officer believes need extension or clarification. In this event, the Hearing Officer shall set forth in writing those issues upon which more evidence is requested, identifying where possible persons or sources from which evidence should be sought. The Manager of Operations shall make every effort through appropriate sources to obtain additional information upon the matters indicated by the Hearing Officer;

(r) A written transcript of the entire proceedings shall be made by a person possessing appropriate DOE clearance and, except for portions containing Restricted Data or national security information, a copy of such transcript shall be furnished the individual without cost.

[42 FR 52382, Sept. 30, 1977, as amended at 46 FR 18171, Mar. 23, 1981; 48 FR 46501, Oct. 13, 1983]

§ 710.28 Recommendation of the Hearing Officer.

(a) The Hearing Officer shall carefully consider the record and the standards set forth herein. In reaching its determination the Hearing Officer shall consider the demeanor of the witnesses who have testified before the Hearing Officer, the probability or likelihood of the truth of their testimony, their credibility, the authenticity and accuracy of documentary evidence, or lack of evidence upon some material points in issue. If the individual is, or may be, handicapped by the non-disclosure to him of confidential information or by lack of opportunity to cross-examine confidential informants, the Hearing Officer shall take that fact into consideration. The Hearing Officer may also consider as part of the record the individual's past employment in the energy research and development program, and the nature and sensitivity of the job he is or may be expected to perform. Possible impact of the loss of the individual's services upon the DOE program shall not be considered by the Hearing Officer;

(b) The Hearing Officer shall make specific findings based upon the records as to whether each of the allegations contained in the notification letter is true or false and the significance which the Hearing Officer attaches to such allegations. These findings shall be supported fully by a statement of reasons which constitute the basis for such findings;

(c) The Hearing Officer's recommendation shall be predicated upon the Hearing Officer's findings. If, after considering all the factors in light of the criteria set forth in this part, the Hearing Officer is of the opinion that it will not endanger the common defense and security and will be clearly consistent with the national interest to grant access authorization to the individual, the Hearing Officer shall make a favorable recommendation; otherwise the Hearing Officer shall make an adverse recommendation.

(d) The Hearing Officer's recommendation shall be submitted to the Manager of Operations, accompanied by a statement of the findings and reasons supporting the Hearing Officer's conclusions within 30 days of the receipt of the hearing transcript by the Hearing Officer, or the closing of the record, whichever is later, unless an extension is granted by the Director, Office of Safeguards and Security.

[42 FR 52382, Sept. 30, 1977, as amended at 46 FR 18171, Mar. 23, 1981; 48 FR 46801, Oct. 13, 1983]

§ 710.29 New evidence.

(a) In the event of the discovery of new evidence by the individual prior to final determination of the individual's eligibility for access authorization, such evidence shall be submitted by the individual or his representative to the Manager of Operations from whom he received the notification letter;

(b) The Manager of Operations with the advice of Hearing Counsel shall review the application for the presentation of new evidence to ascertain its materiality and relevancy and further, that the individual or his representative is without fault in failing to present the evidence before. In the event it is determined that the new evidence should be received, the Manager of Operations shall:

(1) Refer the matter to the Hearing Officer who had been appointed in the individual's case when the Manager of Operations has not yet transmitted the record to the Assistant Secretary for Defense Programs. The Hearing Officer receiving the application for the presentation of the new evidence shall determine the form in which it shall be received, whether by testimony before the Hearing Officer, by deposition, or by affidavit.

(2) In those cases where the Manager of Operations has forwarded the record to the Assistant Secretary for Defense Programs, the application for presentation of new evidence shall be referred to the Assistant Secretary for Defense Programs with appropriate comment and recommendations. In the event the Assistant Secretary for Defense Programs determines that the new evidence should be received, he shall determine the form in which it shall be received, whether by testimony before a Hearing Officer, by deposition or by affidavit.

[42 FR 52382, Sept. 30, 1977, as amended at 46 FR 18171, Mar. 23, 1981]

§ 710.30 Actions on the recommendations.

(a) The signed report of the Hearing Officer containing findings, supporting reasons, conclusions and recommendations, shall be submitted to the Manager of Operations, together with the hearing record, within 30 days of the Hearing Officer's receipt of the hearing transcript or the closing of the record, whichever is later, unless an extension is granted by the Director, Office of Safeguards and Security.

(b) Upon receipt of the findings and recommendation of the Hearing Officer and the record, the Manager of Operations shall forthwith transmit it to the Assistant Secretary for Defense Programs through the Director, Division of Safeguards and Security. In those cases where denial of access authorization is recommended by the Hearing Officer, the Manager of Operations shall forward a statement concerning the effect which denial of access authorization would have upon the energy research and development program.

(c) The Assistant Secretary for Defense Programs may return the record to the Manager of Operations for further proceedings by the Hearing Officer with respect to specific matters designated by the Assistant Secretary for Defense Programs.

(d)(1) In the event a recommendation by the Hearing Officer for a denial of access authorization, the individual shall be immediately notified in writing of that fact by the Assistant Secretary for Defense Programs and shall be informed of the Hearing Officer's findings with respect to each allegation contained in the notification letter. The individual shall also be notified of his right to request a review of his case by the DOE Personnel Security Review Examiner and of his right to submit a brief in support of his contentions. The request for a review shall be submitted to the Assistant Secretary for Defense Programs within five days after the receipt of the notice. The brief shall be forwarded to the Assistant Secretary for Defense Programs through the Director, Division of Safeguards and Security, no later than 10 days after receipt of such notice, unless such time is extended by the Assistant Secretary for Defense Programs for good cause shown;

(2) Where the individual requests a review of the adverse recommendation, the Assistant Secretary for Defense Programs shall forthwith send the record, with all findings and recommendations, to the Personnel Security Review Examiner;

(3) In the event the individual fails to request a review by the DOE Personnel Security Review Examiner of an adverse recommendation within the prescribed time, the final determination shall be made on the basis of the record with all findings and recommendations;

(e) Where the DOE Hearing Officer has made a recommendation favorable to the individual and the Assistant Secretary for Defense Programs proposes to transmit the record to the Personnel Security Review Examiner for its recommendation, the Assistant Secretary for Defense Programs shall immediately cause the individual to be notified of that fact and of those matters contained in the notification letter concerning which he desires the advice of the Personnel Security Review Examiner. The Assistant Secretary for Defense Programs shall further inform the individual that he may submit a brief concerning such matters for the consideration of the Personnel Security Review Examiner. Such brief shall be filed not later than 10 days from the receipt of the notice by the individual, unless extended for good cause shown. The brief shall be forwarded to the Assistant Administrator for National Security for transmission to the Personnel Security Review Examiner.

[42 FR 52382, Sept. 30, 1977, as amended at 48 FR 46501, Oct. 13, 1983]

§ 710.31 Recommendations of the DOE Personnel Security Review Examiners.

(a) The Assistant Secretary for Defense Programs shall designate three DOE Personnel Security Review Examiners to conduct a DOE Personnel Security Review Examination of the record of the case. The designated Examiners shall individually and independently, without consulting or otherwise communicating with one another, consider the matter under review based upon the record supplemented by such brief as the individual submits. Examiners may request such additional briefs as any of them deems appropriate, which will be obtained by the Assistant Secretary for Defense Programs and provided to each Examiner. In any case where an Examiner determines that additional evidence or further proceedings are necessary, the record may be returned to the Assistant Secretary for Defense Programs with a recommendation that the case be remanded to the Manager of Operations for appropriate action, which may include returning the case to the Hearing Officer and reconvening the hearing to obtain additional testimony.

(b) In the Examiner's consideration, each shall make individual findings and recommendations on the record supplemented by additional testimony or briefs as have previously been determined by an Examiner(s) as appropriate. When additional testimony is taken by the Hearing Officer, a verbatim transcript of such testimony shall be made part of the record.

(c) The Examiners shall not consider the possible impact of the loss of the individual's services upon the DOE program.

(d) After consideration, each Examiner shall individually prepare a report of findings and recommendations and submit the report in writing to the Assistant Secretary for Defense Programs. These findings and recommendations shall be fully supported by stated reasons for their conclusions. Except in those cases where the Personnel Security Review Examiners have requested additional information as provided for in paragraphs (a) or (b) of this section, the Personnel Security Review Examiners shall submit their report of findings and recommendations to the Assistant Secretary for Defense Programs within 45 days of their receipt of each case, unless an extension is granted by the Deputy Assistant Secretary for Security Affairs.

[46 FR 18172, Mar. 23, 1981, as amended at 48 FR 46501, Oct. 13, 1983]

§ 710.32 Action by the Assistant Secretary for Defense Programs.

(a) The Assistant Secretary for Defense Programs, on the basis of the record accompanied by all recommendations, shall then make a final determination whether access authorization shall be granted or denied;

(b) In making the determination as to whether access authorization shall be granted or denied, the Assistant Secretary for Defense Programs shall give due recognition to the favorable as well as the unfavorable information concerning the individual and shall take into account the value of the individual's services to the energy research and the development program and the operational consequences of denial of access authorization;

(c) In the event of an adverse determination, the Assistant Secretary for Defense Programs shall notify the individual through the Manager of Operations of his decisions that access authorization is being denied or revoked and of his findings with respect to each allegation contained in the notification letter for transmittal to the individual.

§ 710.33 Action by the Secretary.

(a) Whenever an individual has not been afforded an opportunity to confront and cross-examine witnesses who have furnished information adverse to the individual under the provisions of § 710.27 (m), (n), (o), or (p) and an adverse recommendation has been made by the Assistant Secretary for Defense Programs, the Secretary shall personally review the record and determine whether access authorization shall be granted, denied or revoked, based upon the record;

(b) When the Secretary determines to deny or revoke access authorization the individual will be notified through the Manager of Operations of his decision that access authorization is being denied or revoked and of his findings with respect to each allegation contained in the notification letter for transmittal to the individual;

(c) Nothing contained in these procedures shall be deemed to limit or affect the responsibility and powers of the Secretary to deny or revoke access to Restricted Data, national security information, or significant quantities of special nuclear material if the security of the nation so requires. The Secretary's authority may not be delegated and may be exercised only when the Secretary determines that the procedures prescribed in § 710.27 (m), (n), (o), or (p) cannot be invoked consistently with the national security and such determination shall be conclusive.

§ 710.34 Reconsideration of cases.

(a) Where, pursuant to the procedures set forth in §§ 710.20 through 710.33, the Assistant Secretary for Defense Programs or the Secretary has made a determination granting access authorization to an individual, the individual's eligibility for access authorization shall be reconsidered only when, subsequent to the time of the prior hearing, there is new substantially derogatory information or a significant increase in the scope or sensitivity of the Restricted Data or national security information to which the individual has or will have access;

(b) Where, pursuant to those procedures, the Secretary or the Assistant

Secretary for Defense Programs has made a determination denying access authorization to an individual, the individual's eligibility for access authorization may be reconsidered when there is a bona fide offer of employment requiring access to Restricted Data, national security information or significant quantities of special nuclear material and either material and relevant new evidence which the individual and his representatives are without fault in failing to present before, or convincing evidence of reformation or rehabilitation. Requests for reconsideration shall be submitted in writing to the Assistant Secretary for Defense Programs through the Manager of Operations having jurisdiction over the position for which access authorization is required. Such requests shall be accompanied by an affidavit setting forth in detail the new evidence or evidence of reformation or rehabilitation. The Assistant Secretary for Defense Programs shall cause the individual to be notified as to whether his eligibility for access authorization will be reconsidered and, if so, the method by which such reconsideration will be accomplished;

(c) Where access authorization has been granted to an individual by a Manager of Operations without recourse to the procedures set forth in §§ 710.20 through 710.33, the individual's eligibility for access authorization shall be reconsidered only in a case where, subsequent to the granting of access authorization, new substantially derogatory information has been received or there is a significant increase in the scope or sensitivity of the Restricted Data or national security information to which the individual has, or will have access, and in any other case only with specific prior approval of the Director, Division of Safeguards and Security, DOE.

MISCELLANEOUS

§ 710.35 Terminations.

In the event the individual is no longer an applicant for access authorization or no longer requires access authorization the procedures of this part shall be terminated without a final determination as to his eligibility for access authorization.

§ 710.36 Attorney representation.

In the event the individual is represented by an attorney or other such representative, the individual shall file with DOE a document designating such attorney or representative and authorizing such attorney or representative to receive all correspondence, transcripts and other documents pertaining to the proceeding under this part.

§ 710.37 Certifications.

Whenever information is made a part of the record under the exceptions authorized by § 710.27 (m), (n), (o), and (p), the record shall contain certificates evidencing that the determinations required therein have been made.

§ 710.38 Washington Area cases.

In those cases which may arise involving individuals within the Washington Area of DOE operations the Director, Division of Safeguards and Security shall discharge the functions and responsibilities assigned to Managers of Operations in these procedures.

§ 710.39 Time frames.

Statements of time established for processing aspects of a case under this part are the agency's desired time frames in implementing the procedures set forth in this part. They shall have no impact upon the final disposition of an access authorization by the Assistant Secretary for Defense Programs, and confer no rights upon an individual whose eligibility for, or suspension of, access authorization is being considered.

[48 FR 46501, Oct. 13, 1983]

APPENDIX A—SELECTED PROVISIONS OF THE ATOMIC ENERGY ACT OF 1954, AS AMENDED, SEC. 141 (42 U.S.C. 2161), SEC. 145 (42 U.S.C. 2165), SEC. 161 (42 U.S.C. 2201)

(By authority of the Energy Reorganization acts of 1974 (42 U.S.C. 5814) the Administrator of DOE or his designated representative is to be substituted for the "Commission" and "General Manager" as appropriate.)

Sec. 141. Policy. It shall be the policy of the Commission to control the dissemination and disclosure of Restricted Data in such a manner as to assure the common defense and security * * *

Sec. 145. Restriction. (a) No arrangement shall be made under section 31, no contract shall be made or continued in effect under section 141, and no license shall be issued under section 103 or 104, unless the person with whom such arrangement is made, the contractor or prospective contractor, or the prospective licensee agrees in writing not to permit any individual to have access to Restricted Data until the Civil Service Commission shall have made an investigation and report to the Commission on the character, association, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(b) Except as authorized by the Commission or the General Manager upon a determination by the Commission or General Manager that such action is clearly consistent with the national interest, no individual shall be employed by the Commission nor shall the Commission permit any individual to have access to Restricted Data until the Civil Service Commission shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(c) In lieu of the investigation and report to be made by the Civil Service Commission pursuant to subsection (b) of this appendix, the Commission may accept an investigation and report on the character, associations, and loyalty of an individual made by another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individual by another Government agency based on such investigation and report.

(d) In the event an investigation made pursuant to subsections (a) and (b) of this appendix develops any data reflecting that the individual who is the subject of the investigation is of questionable loyalty, the Civil Service Commission shall refer the matter to the Federal Bureau of Investigation for the conduct of a full field investigation, the results of which shall be furnished to the Civil Service Commission for its information and appropriate action.

(e) If the President deems it to be in the national interest he may from time to time determine that investigations of any group or class which are required by subsections (a), (b), and (c) of this appendix be made by the Federal Bureau of Investigation.

(f) Notwithstanding the provisions of subsections (a), (b), and (c) of this appendix, a majority of the members of the Commission shall certify those specific positions which are of a high degree of importance or sensitivity, and upon such certification, the investigation, and reports required by such provisions shall be made by the Federal Bureau of Investigation.

(g) The Commission shall establish standards and specification in writing as to the scope and extent of investigations, the reports of which will be utilized by the Commission in making the determination, pursuant to subsections (a), (b), and (c) of this appendix, that permitting a person access to Restricted Data will not endanger the common defense and security. Such standards and specifications shall be based on the location and class or kind of work to be done and shall, among other considerations, take into account the degree of importance to the common defense and security of the Restricted Data to which access will be permitted.

(h) Whenever the Congress declares that a state of war exists, or in the event of a national disaster due to enemy attack, the Commission is authorized during the state of war or period of national disaster due to enemy attack to employ individuals and to permit individuals access to Restricted Data pending the investigation report, and determination required by section 145b, to the extent that and so long as the Commission finds that such action is required to prevent impairment of its activities in furtherance of the common defense and security.

Sec. 161. General provisions. In the performance of its functions the Commission is authorized to:

(a) Establish advisory boards to advise with and make recommendations to the Commission on the legislation, policies, administration, research and other matters; Provided, That the Commission issues regulations setting forth the scope, procedure, and limitations of the authority of each such board.

(b) Establish by rule, regulation, or order, such standards and instructions to govern the possession and use of special nuclear material, and byproduct material as the Commission may deem necessary or desirable to promote the common defense and security or to protect health or to minimize danger to life or property.

(c) Make such studies and investigations, obtain such information, and hold such meetings or hearings as the Commission may deem necessary or proper to assist it in the administration or enforcement of this Act, or any regulations or orders issued thereunder. For such purposes the Commission is authorized to administer oaths and affirmations, and by subpoena to require any person to appear and testify, or to appear and produce documents, or both, at any designated place. No person shall be excused from complying with any requirements under this paragraph because of his privilege against self-incrimination, but the immunity provisions of the compulsory Testimony Act of February 11, 1893, shall apply with respect to any individuals who specifically claims such privilege. Witnesses subpoenaed, under this subsection, shall be paid the same fees and mileage as are paid witnesses in the district courts of the United States.

* * * * *

(i) Prescribe such regulations or orders as it may deem necessary (1) to protect Restricted Data received by any person in connection with any activity authorized pursuant to this Act, (2) to guard against the loss or diversion of any special nuclear material acquired by any person pursuant to section 53 or produced by any person in connection with any activity authorized pursuant to the Act, to prevent any use or disposition thereof which the Commission may determine to be inimical to the common defense and security, including regulations or orders designating activities, involving quantities of special nuclear material which in the opinion of the Commission are important to the common defense and security, that may be conducted only by persons whose character, associations, and loyalty shall have been investigated under standards and specifications established by the Commission and as to whom the Commission shall have determined that permitting each person to conduct the activity will not be inimical to the common defense and security, and (3) to govern any activity authorized pursuant to this Act, including standards and restrictions governing the design, location, and operation of facilities used in the conduct of such activity in order to protect health and to minimize danger to life or property;

* * * * *

(n) Delegate to the General Manager or other officers of the Commission any of those functions assigned to it under this Act except those specified in sections 51, 57b., 61, 108, 123, 145b. (with respect to the determination of those persons to whom the Commission may reveal Restricted Data in the national interest), 145f. and 161a.

* * * * *

(p) Make, promulgate, issue, rescind, and amend such rules and regulations as may be necessary to carry out the purposes of this Act.

[43 FR 52388, Sept. 30, 1977]

purchase price is of such a magnitude compared to the cost of installation as to distort the amount of technical direction and management effort required of the contractor. Generally, special equipment is considered to be a capital-asset-type of equipment (typically equipment costing more than $1,000 and having a service life of more than two years) for which the cost of installation and handling (including unloading, hauling and warehousing) is 5%, or less, of the purchase price of the equipment. However, the determination of specific items of equipment in this category requires application of judgment and careful study of the circumstances involved in each project. This category of equipment would generally include:

(1) Major items of prefabricated process or research equipment.

(2) Major items of preassembled equipment such as packaged boilers, generators, machine tools, and large electrical equipment. In some cases, it would also include special apparatus or devices such as reactor vessels and reactor charging machines.

970.1509-8 Special considerations—award fee.

(a) When a management and operating contract is to be awarded on an award-fee basis, several special considerations are appropriate.

(b) In management and operating contracts, the base fee portion of the fee objective should not normally exceed 50% of the otherwise applicable fixed fee. However, the base amount may range from 0 to 50% of the fixed fee amount. In the event 50% is exceeded, appropriate documentation shall be entered into the contract file. In no event shall the base fee exceed 60% of the fixed fee amount.

(c) The base fee plus the amount included in the award fee pool should normally not exceed the fixed fee (as subjectively determined or as developed from the fee schedule) by more than 50%. However, in the event that the base fee is to be less than 50% of the fixed fee, the maximum potential award fee may be increased proportionately with the decreases in base fee amounts.

(d) The following maximum potential award fees shall apply in award fee contracts: (percent is stated as percent of fee schedule amounts).

Base fee (percent)	Award fee (percent)	Maximum total (percent)
50	100	150
40	120	160
30	140	170
20	160	180
10	180	190
0	200	200

(e) Prior approval of the Procurement Executive, is required for total fee (based plus award fee pool) exceeding the guidelines in paragraph (d), above. Additionally, in the event use of the award fee guidelines in (d), above, result in total fees which exceed or are expected to exceed the statutory limitations imposed by 10 U.S.C. 2306(d) and 41 U.S.C. 254(b), prior approval of the Procurement Executive shall be obtained.

Subpart 970.19—Small Business and Small Disadvantaged Business Concerns

970.1901 General.

(a) The policies and procedures in the following FAR sections shall be applied to the acquisition activities of management and operating contractors.

19.301, 19.302, 19.502-2, 19.503-3, 19.508(b), 19.508(c), 19.508(d)

(b) Protests received by management and operating contractors regarding small business status or questions concerning small disadvantaged business shall be referred to the Small Business Administration through the DOE contracting officer.

(c) Procurements of $10,000 or less awarded through small purchase procedures shall be reserved exclusively for small business where there is a reasonable expectation that bids will be obtained from two or more responsible small business concerns that are competitive with market prices, quality and delivery.

(d) Acquisition by management and operating contractor of construction estimated to cost $3 million or less, including new construction, and repair and alteration of structures, shall be required to be set aside on a class basis for small business concerns. When, in the judgment of the contractor, a particular acquisition falling within these dollar limits is determined to be unsuitable for a small business set-aside, notification to SBA shall be made through the DOE contracting officer. Unless SBA appeals the decision, the contractor shall proceed to process the acquisition on an unrestricted basis. Small business set-aside preferences should be considered on a case-by-case basis, for acquisition of construction in excess of $3 million favoring the preferential participation of small business, whenever appropriate.

(e) Initiation of set-asides by contractors shall be made on a unilateral basis.

(f) Contracting activities shall require management and operating contractors to prepare quarterly reports on small business, small disadvantaged business, women-owned small business and contracts placed in labor surplus areas.

(g) To expand participation of small and small disadvantaged business sources, management and operating contractors shall publicize proposed actions of $100,000 and above in accordance with FAR subpart 5.2. This procedure will be followed unless approval by the contracting officer to waive the requirements of this provision is obtained.

(h) The clause at FAR 52.219-9 as modified by 952.219-9 shall be included in management and operating contracts.

Subpart 970.20—Labor Surplus Area Concerns

970.2001 General.

(a) Management and operating contractors shall be authorized to employ total labor surplus area (LSA) set-asides where there is a reasonable expectation that bids or proposals will be obtained from a sufficient number of responsible LSA concerns so as to ensure that awards will be made at reasonable prices. The priorities set forth in FAR 19.504 shall be utilized in determining the type of set-aside to be employed.

(b) Protests received or questions raised by contractors regarding LSA status shall be handled with the Department of Labor through the DOE contracting officer.

(c) LSA set-aside acquisitions awarded by management and operating contractors shall be reported quarterly in accordance with "A Guide to Preparation of DOE Quarterly Procurement and Financial Assistance Reports."

(d) Initiation of set-asides by management and operating contractors shall be on a unilateral basis.

Subpart 970.22—Application of Labor Policies

970.2201 Basic labor policies.

(a) Contracting officers shall in appropriate circumstances, follow the guidance in FAR subpart 22.1 except as provided below in award and management of management and operating contracts.

(b) The extent of Government ownership of the nation's energy plant and materials, and the overriding concerns of national defense and security, impose special conditions on personnel and labor relations in the energy program, namely, continuity of vital operations at DOE installations must be assured; DOE must retain absolute authority on all questions of security; DOE reviews labor expenses under management and operating contracts as a part of its responsibility for assuring judicious expenditure of public funds. It is the intent of DOE, that personnel and labor policies throughout the energy program should reflect the best experience of American industry in aiming to achieve the type of stable labor-management relations essential to the proper development of the energy program. The following enunciates the principles upon which the DOE policy is based:

(1) *Employment standards.* (i) Management and operating contractors are expected to bring experienced, proven personnel from their private operations to staff key positions on the contract work and to recruit other well-qualified personnel as needed. Such personnel should be employed and treated during employment without discrimination by reason of race, color, religion, sex, or national origin. Contractors shall be required to take affirmative action to achieve these objectives.

(ii) The job qualifications and suitability of prospective employees should be established by the contractor prior to employment by careful personnel investigations. Such personnel investigations should include, as appropriate: a credit check; verification of high school degree/diploma or degree/diploma granted by an institution of higher learning within the last 5 years; contacts with listed personal references; contacts with listed employers for the past 3 years (excluding employment of less than 60 days duration, part-time employments, and craft/union employments); and local law enforcement checks *when* such checks are not prohibited by state or local law, statute, or regulation, and when the individual had resided in the jurisdiction where the contractor is located. Where a security clearance will be required, the applicant's job qualifications and suitability must be established before a request is made to DOE for a security clearance. When an applicant is being hired specifically for a position which shall require a DOE security clearance, the applicant shall not be placed in that position prior to the security clearance being granted by the DOE unless an exception has been obtained from the Head of the Contracting Activity or designee.

(iii) The contractor is responsible for maintaining satisfactory standards for employee qualifications, performance, conduct, and business ethics under its own personnel policies.

(2) *Security.* On all matters of security at its installations, DOE retains absolute authority and neither the security rules nor their administration are matters for collective bargaining between management and labor. Insofar as DOE security regulations affect the collective bargaining process, the security policies and regulations will be made known to both parties. To the fullest extent feasible, DOE will consult with representatives of management and labor in formulating security rules and regulations that affect the collective bargaining process.

(3) *Wages, salaries, and employee benefits.* (i) Wages, salaries, and employee benefits shall be administered in a manner designated to adapt normal industry or university practices and conditions to the contract work and to provide for appropriate review by DOE. Area practices, valid patterns, and well-established commerical or academic practices of the contractors, as appropriate, form the criteria for the establishment and adjustment of compensation schedules.

(ii) The aspects of wages, hours, and working conditions which are the substance of collective bargaining in normal organized industries will be left to the orderly processes of negotiation and agreement between DOE contractor managements and employee representatives with maximum possible freedom from Government interference.

(4) *Employee relations.* The handling of employee relations on contract work, including such matters as the conduct and discipline of the work force and the handling of employee grievances, is part of the normal management responsibility of the contractor.

(5) *Collective bargaining.* (i) DOE review of collective bargaining practices will be premised on the view that management's trusteeship for the operation of the Government facilities includes the duty to adopt practices which are fundamental to the friendly adjustment of disputes, and which experience has shown promote orderly collective bargaining relationships. Practices inconsistent with this view may be objected to, if not found to be otherwise clearly warranted.

(ii) In line with the policy of assuring continuity of operation of vital facilities, all collective bargaining agreements at Government-owned energy installations should provide that grievances and disputes involving the interpretation or application of the agreement will be settled without resorting to strike, lockout, or other interruption to normal operations. For this purpose, each collective bargaining agreement should provide an effective grievance procedure with arbitration as its final step, unless the parties mutually agree upon some other method of assuring continuity of operations for the term of the agreement.

(iii) DOE expects its management and operating contractors and the unions representing contractor employees to cooperate fully with the Federal Mediation and Conciliation Service.

(6) *Personnel training.* DOE encourages and supports personnel training programs aimed at improving work efficiency or developing needed skills which are not otherwise obtainable.

(7) *Working conditions.* Accident, fire, health, and occupational hazards associated with DOE activities will be held to a practical minimum level and controlled in the interest of maintenance of health and prevention of accidents. To this end, contractors shall be required to maintain comprehensive continuous preventive and protective programs appropriate to the particular activities throughout all operations subject to DOE control. Appropriate financial protection in case of occupational disability must be provided employees on DOE projects.

(c) Title to payroll and associated records under certain contracts for the management and operation of DOE facilities, and for necessary miscellaneous construction incidental to the function of these facilities, shall vest in the Government. Such records are to be disposed of in accordance with DOE directions. For such contracts, the Solicitor of Labor has granted a tolerance from the Department of Labor Regulations to omit from the prescribed labor clauses the requirement for the retention of payrolls and associated records for a period of three years after completion of the contract. Under this tolerance, the records retention requirements for all labor clauses in the contract and the Fair Labor Standards Act is satisfied by disposal of such records in accordance with DOE directives.

970.2202 Convict labor.

The provisions of FAR Subpart 22.2 shall apply to procurement by management and operating contractors.

Comparison: Background Investigations by OPM and DIS

Position		OPM	DIS	Update Required	
Sensitivity (OPM Designation)	Access	(Civilian Competitive Service, Excepted Service Where Requested by Agency)	(DOD Civilian, Military, DOD Govt. Contractors)	OPM	DIS
Non-sensitive	None	NACI (National Agency Check w/ Inquiries)--covers past 5 yrs. through written inquiry to employers, schools, references, and law enforcement.	N/A	None	None
Non-critical sensitive	Confidential	Expanded NACI or MBI (Minimum Background Investigation)--covers past 5 years.	NAC (National Agency Check) --written check indices (FBI and DOD, where appropriate INS, CIA, State Department, federal law enforcement).	None	None
Non-critical sensitive	Secret	LBI (Limited Background Investigation)--personally-conducted field inquiry on past 3 years, written inquiry on 2 years beyond.	NAC (same as above)	None	Every 5 years required - in practice DIS is doing no secret updates due to manpower restrictions.
Critical-sensitive	Top-Secret	BI (Background Investigation)--personally-conducted field inquiry on past 5 years, written inquiry for 2 years beyond.	For DOD civilian personnel --BI (standard background investigation)--field coverage of past 5 years on employment, education, references, credit, criminal records. For military and contractor personnel--IBI (interview oriented investigation)--NAC, local agency, credit checks, references and subject interview.	Recommend agency require every 5 yrs. - OPM now performs as requested by agency.	Every 5 years required - in practice DIS is unable to meet quota of 40,000/yr. for TS/SCI updates -- currently doing SCI updates where resources allow.
Special-sensitive	Special Compartmented Information (SCI)	SBI (Special Background Investigation)--field background covering past 15 years (as required by CIA directive).	SBI (Special Background Investigation)--similar to BI but covers past 15 years (as required by CIA directive).	Recommend agency require every 5 yrs. - OPM now performs as requested by agency.	

STATEMENT OF

JEREMIAH M. DOLAN
CORPORATE DIRECTOR OF SECURITY & ADMINISTRATIVE SERVICES
AEROJET GENERAL

AND

INDUSTRY ADVISOR
INDUSTRIAL SECURITY REVIEW COMMITTEE

BEFORE THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

AT HEARINGS ON

U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM

APRIL 1985

STATEMENT

To introduce myself:

I am Jerry Dolan and I'm here today in my capacity as industry advisor to the Industrial Security Review Committee which was formed as a result of the James Durwood Harper espionage case. I also serve as Chairman of the Industrial Security Committee of the Aerospace Industries Association which serves as an interface between security representatives of major aerospace corporations and government policy officials to resolve problems of mutual interest.

I am employed by Aerojet General Corporation of La Jolla, California as the Corporate Director of Security and Administrative Services. I previously served with the FBI for twenty-seven years.

With respect to industrial security issues, as the industry advisor to the so-called Harper Committee, I have had an opportunity to assist in formulating various recommendations resulting from one year's investigation into the current industrial security system.

In my view, some of the most positive and far-reaching changes recommended have to do with the revised scope of personnel security investigations and the enhancements of investigative standards.

For example, in past years most secret clearances were granted on the basis of a favorable national agency check(NAC) alone.

The committee has recommended adding local agency checks and credit and employment reviews to the NAC, thus making the secret clearance investigation far more comprehensive.

In addition, it has been recommended that the delays in awarding clearances be substantially reduced through administrative procedures that pose limited risks. These changes would remove a problem most defense contractors have experienced, because now, recently hired skilled employees would be able to function effectively with a clearance while the investigative process is proceeding. If this recommendation is approved, the productivity gains would be considerable.

Two other factors should be be taken into account in evaluating this recommendation: The "at risk" period, if a clearance is granted at the beginning of the investigation, is approximately 60 to 120 days. It is fair to say, espionage is usually conducted by those who are familar with security procedures, not by someone new to the classified arena. Therefore the vulnerability aspect is clearly manageable. Secondly, the clearance rejection rate currently stands at only .06 of those who apply. These are certainly tolerable numbers.

The committee also feels a new system of DIS authority, granting on-the-spot upgrades of security clearances with reasonable safeguards, is a proper device with minimal hazards.

I have also expressed to the committee, certain reservations on some issues that it has approved, e.g. the establishment of a hot line; the creation of a DIS advisory role to provide assistance to defense contractors above and beyond the normal inspectors; and an expanded rating system for government inspections of contractors. In my opinion though, these issues are not of major negative significance.

Of much more importance is the realization, held by most responsible security people today, that the funds allocated for industrial security protections are being disbursed in the right direction.

The weaknesses in the industrial security system that have surfaced and hurt us badly have come from cleared persons with legitimate access to classified information at their facilities who have turned sour. I don't recall any cases in recent history where classified material has been spirited out of a facility by individuals with no legitimate clearance access. The weakness does not lie in inadequate physical security. It comes, for the most part, from cleared personnel who are greedy.

The Defense Investigative Service is now spending dollars to attempt to improve this situation by conducting periodic re-investigations of cleared personnel who have access to sensitive material.

There is no foolproof system available in a democratic society that will totally preclude individuals from cooperating with a hostile intelligence service while employed in the defense business. The best we can hope for is a system of controls that will serve as a reasonable deterrent against taking that first step toward committing espionage.

How do we accomplish this? How can we decrease the odds of another Boyce, Bell or Harper?

Periodic reinvestigations, as cited above, are positive and effective techniques.

Frequent reminders to cleared employees of their adverse information responsibilities will also be helpful.

In addition, there is research currently being conducted, under government auspices, to chemically treat paper in such a way that classified documents being illegally transported out of a facility would be detected by monitoring devices.

Granted, these devices would have to be low-cost, distributed on a large scale, and designed to defeat the Xerox copier.

So far this research has failed to produce these products on a cost-effective scale, however, this concept has been successfully applied to some very special situations. I believe this type of control would dissuade defense employees from illegally removing classified data. Certainly, it would add to the effectiveness of spot-searches of briefcases and the like now utilized by some contractors.

Another addition to expanded deterrent may be the use of behavioral testing and the application of the polygraph to a greater degree. Neither is perfect, but these two techniques could certainly add to the effectiveness of our programs.

We should also spend more dollars in the general field of security education. There is movement in this direction at present, but more emphasis is needed to ensure that current "awareness" messages are effectively conveyed to defense employees.

Another item for consideration would be to increase the number of contracts being let that include security incentives. Care must be taken, however, to ensure these incentives are not provided on a routine basis but only when extra and innovative security measures are needed.

Concerning physical security, it is unfortunate that today there is a body of opinion within the government that suggests proprietary or "in-house" security guards should be replaced by contract guard forces. The U.S. Government spends untold sums to manufacture products of the utmost sensitivity to our defense effort and yet the protection of these assets, in the eyes of some, should be turned over to contract guards purely for cost reasons. I believe this is false economy at its worst.

This subcommittee has already been provided with position papers from industry on this topical problem. Included among the reasons cited for not opting for contract guards is the erosion of management/labor relationships that have been built up over the years. The threat of labor unrest could be a very real possibility if these dramatic changes of personnel occur.

Another area, communications security, is also an integral part of the defense industry protection package. The National Security Agency has recently funded research that could result in the availability of hardware at reasonable cost to protect our voice and data transmissions both in the classified and unclassified/sensitive areas. Previous equipment was either not available or far too expensive for wide acceptance in industry.

Communications security seems to be solving some of its problems. New legislation has also been proposed to limit the intercept capabilities of hostile intelligence services through diplomatic expulsions. That, along with a more reasonable and balanced position on the imposition of Tempest requirements (electronic emanations), will better serve our needs and provide far less expenditures in minimal risk programs.

I believe these suggestions, along with the recommendations of the Harper Committee, should help in improving the industrial security program.

In closing, since joining the ranks of industrial security practioners some six years ago, I've been impressed with the dedication of the people involved in protecting our technology.

The tools to accomplish this end are better than they were. Funds are being allocated in the correct directions -- thanks to re-evaluations of priorities by both government and industry.

I'm confident we can and will do better in the future.

STATEMENT OF

CENTRAL INTELLIGENCE AGENCY

BEFORE THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

AT HEARINGS ON

U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM

MARCH 1985

THE PERSONNEL SECURITY PROGRAM OF THE CENTRAL INTELLIGENCE AGENCY

I. BACKGROUND

- The personnel security program at the Central Intelligence Agency has developed over many years and represents the cumulative thinking and judgments of many individuals. The personnel security policies and procedures are designed to prevent the penetration of the Agency. A strong and viable personnel security program is not totally dependent upon the Agency's Office of Security standing alone. It is vital to involve and have coordination and cooperation with other elements of the Agency, particularly the Offices of Personnel and Medical Services, which share major responsibilities in the screening area.

- Personnel security demands allocation of more than half of the Office of Security's resources. These officers are dedicated to the areas of prescreening, investigation, adjudication, polygraph, security awareness, security troubleshooting, and reinvestigation/repolygraph. The personnel security function is supported by a network of strategically located field offices, and in-house polygraph capability, and a small counterintelligence unit.

- In a sense, the Office of Security is a watchdog for the Director of Central Intelligence. The watchdog in this case ensures that the activities of the Agency are carried out in a manner that protects personnel, sources of information, methods of operations and protects classified intelligence information. In all of this there is no function more important than personnel security, which might properly be defined as the program that seeks to ensure that the Agency always employs and is associated with people who can be trusted with the Nation's top secrets.

II. PERSONNEL SECURITY STANDARDS/AUTHORITIES

- The Agency's investigative and adjudicative authorities are set out in the National Security Act of 1947 and the CIA Act of 1949. These authorities were expanded upon in Executive Orders 10450 and 12036, various Agency regulations and Director of Central Intelligence Directive 1/14.

- Agency regulations state in part that it is imperative that Agency personnel be persons "who are of excellent character, and of unquestioned loyalty, integrity, discretion, and trustworthiness." That was lifted out of 10450, and the

Agency's standards are high because CIA's mission is vital to national security and much is expected of those who carry it out. The Agency necessarily insists on standards of integrity, personal responsibility, trustworthiness and loyalty well beyond what most other employers demand.

III. OFFICE OF PERSONNEL SCREENING

° The Agency's Office of Personnel recruiters fill the Agency's personnel needs by utilizing direct newspaper advertising or contacts with appropriate sources in universities, military bases, private industry, vocational/technical institutions, or the referrals of current and former employees. These recruiters are scattered throughout the United States.

° Once the applicant is located and identified, initial interviews are arranged with the recruiter. The most promising candidates are asked to submit resumes and, in most cases, the recruiter arranges for a professional applicant test battery to be administered. The recruiter will then send to Headquarters his interview report, along with his recommendation.

° A key step in the process involves the use of expediters who are experienced professional security officers assigned to the Office of Personnel. The expediters painstakingly review the Personal History Statement submitted by the applicant, concentrating on entries that tend to signal trouble--the items most likely to be falsified by the candidate. The expediters then attempt to contact all the applicants put into processing in order to identify and eliminate those individuals who have made admissions which soundly establish their unsuitability for Agency employment or who will do so in a telephone interview--normally about ten percent of the candidates.

IV. OFFICE OF MEDICAL SERVICES SCREENING

° All applicants are required to complete medical processing prior to entry on duty. This processing consists of a medical evaluation, psychiatric screening, and in some cases psychological assessments. The medical evaluation which consists of accepted and usual medical testing techniques, is appraised by a medical doctor who determines whether the applicant is physically qualified for employment.

° Psychiatric screening begins with the receipt and review of the applicant's report of medical history. Should pertinent psychiatric information be noted, the report is forwarded for special evaluation. Depending upon the nature and extent of the information, the Office of Medical Services may request additional information from the physician of the applicant.

- During the applicant's Headquarters processing, he or she will complete a psychiatric history questionnaire. This is carefully screened by a psychometrist. Depending on the nature of the information developed, or existing recommendations in the file, the psychometrist may refer the applicant for psychiatric interview. A report of the interview will be prepared, reviewed and analyzed by professional staff members and an appropriate recommendation for disposition will be forwarded through command channels.

- Psychological assessments may be requested by operating officials and are mandatory in a number of cases. The assessments are not for medical screening, but are used to match the skills of the applicant with his projected assignement. They may contain significant information as to the suitability and flexibility of the candidate.

V. THE BACKGROUND INVESTIGATION

- Security processing includes the scheduling and conduct of a full field investigation. The investigation is designed to establish the applicant's bona fides and determine that he or she is of excellent character, of unquestioned loyalty, integrity, discretion and trustworthiness. Appropriate National Agency Checks are always conducted, and the field investigation covers the most recent 15 years of the applicant's life, or back to age 17, whichever is shorter.

- All education, employments, and neighborhoods are covered; teachers, fellow students, supervisors, co-workers, and neighbors are interviewed to the extent possible. In addition, a minimum of five character references, including peers, are interviewed. Police checks are conducted on all areas where the applicant has lived, worked or attended school, and credit reputation is established through interviews and/or credit reporting agencies. Suitability and security factors explored by the investigator include family background, reputation and loyalty of spouse and close relatives, as well as the applicant's health, habits, associates, morals, loyalty, financial standing, abilities, personality, character traits, and foreign travels.

- In summary, the background investigation explores every legitimate facet of an applicant's life. The field inquiry by the Office of Security is one of the most comprehensive in Government today. It is closed only when all information, favorable or unfavorable, is confirmed, consolidated and sufficient to permit an equitable decision--fair to the individual and fair to the Agency.

VI. THE POLYGRAPH PROGRAM

° The CIA polygraph program is closely controlled and managed by the Office of Security, following strict guidelines established by the Director of Central Intelligence. Polygraph examiners are generally selected from the ranks of professional security officers who have had on-the-job experience. All examiners are volunteers and are carefully selected for their maturity, emotional stability, evenhandedness and dedication. They receive their three-month formal training at the CIA Polygraph School and then must complete a nine-month probationary period under the close scrutiny of experienced Agency examiners.

° Polygraph testing has played a crucial role in the Central Intelligence Agency's security program for the past 35 years. During this time, the CIA has developed incontrovertible evidence of the value of this vital procedure.

° The CIA's experience with polygraph involves over 128,000 cases and close to a million separate polygraph charts. The value of the polygraph, indeed its indispensability, is clearly reflected in the high number of security disapproval decisions taken by the Director of Security based on information developed during the polygraph examination.

° In the polygraph interview, only those basic questions necessary to satisfy legitimate security concerns are asked. No unrelated information is solicited along the way. Over and above the initial training and probationary period, a strict quality control program is designed to ensure that the highest technical standards are met by examiners, whether at the apprentice or senior examiner level.

VII. THE ADJUDICATION PROCESS

° The basic security responsibility for collating all of the essential data on an applicant rests with the appraiser who ensures that the investigation is complete, and that all appropriate issues are covered in the course of the polygraph interview. This Personnel Security Officer summarizes all the essential elements of the case, and makes an appropriate recommendation in terms of approval, security disqualification, or referral to the Office of Personnel's Applicant Review Panel on suitability grounds.

° The adjudicative phase of security processing is delicate and critical for all concerned. Subjectivity in the process must be reduced to an absolute minimum. Each case is analyzed by an appraiser who has the freedom to vote his or her conscience in making an appropriate recommendation--with no pressure from above. In all cases the total person is considered in order to present a balancead picture which covers both the favorable aspects of an applicant's background as well as problem areas.

° It is a system of checks and balances. Each case is reviewed by a number of senior experienced Security Officers where there is serious derogatory information and a negative recommendation is being made. The final decision is made by the Director of Security who must weigh the evidence, keeping in mind national security above all other considerations. Statistically, over twelve percent of the applicants put into processing are disapproved on strictly security grounds.

VII. THE APPLICANT REVIEW PANEL

° A truly effective personnel screening program involves a team effort by the Offices of Personnel, Medical Services, and Security. This collegial approach to the screening of candidates for employment is best reflected in the work of the Applicant Review Panel, which was established in 1953 to appraise all significant suitability information available through the Agency screening procedures. Data is shared among the Applicant Review Panel members, and is subjected to systematic adjudication before a decision affecting employment is made.

° Adverse suitability information coming within the purview of the Applicant Review Panel may be illustrated as follows: emotional instability and immaturity, personality idiosyncrasies, limited mental capacity including scholarship deficiencies, physical impairment, limitations precluding adaptability and flexibility, poor employment record, financial irresponsibility, including spending habits, excessive alcohol use, and marital difficulties.

° A representative of any one of the three offices may refer a case to the Applicant Review Panel based on suitability information developed during the course of the screening process. It may be data of such a nature that standing alone it does not justify an applicant's rejection, but when related with data existing in other offices, it may acquire greater significance. The Applicant Review Panel is chaired by the Office of Personnel representative and the Panel makes recommendations to the Director of Personnel, who makes the decision to accept or reject the applicant's employment with the Agency. Approximately five percent of the applicants put into processing are disapproved by the Applicant Review Panel because of suitability factors.

IX. THE REINVESTIGATION/REPOLYGRAPH PROGRAM

° In making personnel security decisions, the premise is followed that the past is the precursor of the future. Behavior that is characteristic of a person's background tends to be repeated in the future. In hiring and clearing people, the emphasis is on learning as much as possible about their past. The emphasis on the total person--expensive and time-consuming though it is--pays dividends.

° People do change with time. The applicant hired today will be a significantly different person--physiologically and psychologically--ten years from now. If the "whole person concept" is the key to the initial clearance effort, then the "dynamic person concept" is equally important in the personnel security concerns held about on-duty personnel. A strong personnel security program has to be an on-going effort.

° In view of the sensitive intelligence and counterintelligence mission of the Agency and in support of the statutory responsibility of the Director of Central Intelligence to protect intelligence sources and methods, the Agency has historically and traditionally maintained a program for the periodic review of security cases, as required by DCID 1/14. At the present time there is a review of the status of new employees within the three-year probationary period, and this normally involves both a reinvestigation and a repolygraph. There is also the regular reinvestigation program that follows thereafter on a cycle of every five years.

X. CONCLUSION

° It is the position of the Office of Security that, by and large, the Central Intelligence Agency is composed of very dedicated, hardworking, and capable employees. The screening offices have served jointly as an effective machine in bringing on board individuals of high caliber and diverse backgrounds who possess an extremely wide variety of education, skill, and experience. At the same time, the machine screens out those persons who do not meet Agency security and suitability standards.

EDWIN G. MOORE

BACKGROUND ON THE CASE

Edwin G. Moore, II, was a CIA staff employee from 1952 to 1963 when he was terminated by the DCI after being convicted of arson. He was reinstated in 1967, following acquittal from this charge. He retired in 1973 on medical disability. His career had been marked by marginal work performance, chronic work frustrations and a general reputation of being miscast in an intelligence agency.

In December 1976, Moore threw a package containing classified CIA documents and ransom payment instructions for $200,000 over a fence into a Soviet residence compound. The Soviet watchman was afraid that the package was a bomb and turned it over to a police officer. A subsequent search of Moore's house turned up ten boxes of CIA classified documents dating back to the late 1950s.

In May 1977, Moore was convicted on two counts of espionage and three counts of unlawful possession of classified Government documents. He was sentenced to 15 years imprisonment. He was paroled in 1979.

LESSONS OF CASE/CORRECTIVE ACTIONS

- The Moore case pointed out the need for greater emphasis on the reinvestigation/repolygraph programs and the need to dedicate more resources to such efforts. Following the Moore disclosures, the Agency applied additional resources and took steps to implement reinvestigations and repolygraphs of staff personnel at roughly five-year intervals.

- The Moore case illustrated a need for meaningful reindoctrination and security awareness programs. Again the Agency responded by directing additional resources toward the problem. A new mandatory security reindoctrination program was developed and presented to all employees. In addition, the initial security briefing for new employees was revised and expanded.

- The Moore case demonstrated that first-line supervisors must assume a large responsibility for recognizing and dealing with employee suitability issues before they become security problems. In the Agency, steps were taken through approved training mechanisms to educate the Agency's supervisors about these important duties and responsibilities.

° The Moore case showed that there was a need to generate a greater awareness of the Personnel Evaluation Board (PEB): an interoffice panel consisting of officers from the Offices of Personnel, Security and Medical Services who meet with management representatives to discuss problems of employee suitability. Special efforts were introduced after Moore to publicize the role of PEB and to encourage greater use of the instrumentality. As a result of these efforts, the use and effectiveness of the PEB have increased significantly.

° The Moore case surfaced the need for periodic unannounced spot checks of briefcases and packages to lessen the possibility of unauthorized removal from Agency buildings of classified materials. A special educational program alerted all employees to their physical security responsibilities.

° The Moore case delivered up a more forceful approach in the handling of the Agency's personnel security cases.

° The Moore case reaffirmed that formal compartmentation and need-to-know are viable principles for use in the Agency's security program. This message was transmitted throughout the Agency.

° The Moore case showed that there is close interrelationship between security and suitability issues: a disgruntled employee has the potential for causing serious security difficulties regardless of the basis for his bitterness. After the Moore case, this point was made with unusual vigor throughout the chain of command and with those involved with clearance adjudications.

° The Moore case showed that Agency management had to place greater reliance on the screening arms of the Agency, particularly the Office of Medical Services which was quite accurate in its psychological assessment of Mr. Moore. The Office of Medical Services now plays a stronger role in the screening of applicants.

° The analysis of the Moore case concluded that a vigorous repolygraph program offers the best chance of uncovering an individual who is deliberately violating the security trust expected of employees. The Agency's repolygraph program was significantly strengthened as a result of the Moore case review.

• The Moore case led to the conclusion that the cornerstone of a sound security program is faith and trust in the individual employee. The quality of employees should be uppermost in the selection process. Personnel security standards must not be bent.

CHRISTOPHER BOYCE

BACKGROUND ON THE CASE

Christopher John Boyce worked for TRW, Inc., in El Segundo, California, from 1974 to 1976 as a document control clerk, courier and communicator. He had access to Agency classified and compartmented documents regarding technical intelligence collection systems, and to cryptological systems. During Boyce's employment at TRW, he periodically removed, copied and returned hundreds of documents. He photographed other documents and devices in the document control and communications center where he worked. Boyce gave this information to an accomplice, Andrew Daulton Lee, who sold it to the Soviets for about $76,000.

In January 1977, the Mexican police arrested Lee outside the Soviet Embassy in Mexico City. He was found to have microfilms of Top Secret documents in his possession. Boyce and Lee were convicted of conspiracy, espionage, and theft. Boyce was sentenced to 40 years imprisonment, and Lee to life imprisonment.

LESSONS OF THE CASE/CORRECTIVE ACTIONS

- The Boyce case illustrated a need to initiate a program of selective polygraph use in private industry on key contractor personnel having access to sensitive codeword documents. In the Agency an authorization was obtained for a pilot effort which later led to a formal approval to establish an industrial polygraph program.

- The Boyce case showed that investigative coverage in industrial cases should be as extensive as in staff cases and should focus on peer connections in addition to family associations. This message was transmitted to all Agency field office investigative personnel.

- The Boyce case determined that the application of personnel security standards in the appraisal of industrial cases had to be upgraded to the level of adjudication used in Agency staff employee cases. After Boyce, steps were immediately taken to tighten the screening process in contractor cases.

- The Boyce case surfaced a need for a program of periodic, unannounced, comprehensive security audits of industrial contractor facilities. Resources were obtained to establish an Industrial Security Branch with the responsibility of conducting these security inspections.

- The Boyce case brought home again the close relationship between security and suitability issues in the realm of personnel security. The personality and character flaws of Christopher Boyce were the key to his treasonable behavior in private industry. In the wake of the case, the Agency moved to a greater emphasis upon suitability issues in the industrial cases. In addition, a new Industrial Review Panel was created at that time to address suitability problems in industry.

- Though essentially a personnel security failure, the Boyce case also led to various physical security reform measures, especially having to do with document controls and personnel access controls.

- The Boyce case pointed to the need to improve the line of communication between the Agency and the industrial security officer counterparts. Arrangements, therefore, were made to hold regularly scheduled Industrial Security Seminars to educate contractor security officers on Agency security requirements, and to provide a forum for appropriate dialogue on matters of mutual interest.

- The Boyce case again showed the correlation between effective line supervision and effective security. It also illustrated the importance of involvement by all supervisors in the policies and practices of the Organization's security program.

- The Boyce case delivered insights on necessary security reforms for communications and registry operations, especially the "two-man" rule whenever handling especially sensitive information is involved.

WILLIAM KAMPILES

BACKGROUND ON THE CASE

William Peter Kampiles was a CIA staff employee from March until October 1977. In approximately August 1977, he removed a Top Secret/compartmented manual pertaining to a sensitive technical collection project. He removed it from the office where he was assigned, walked out of the Agency Headquarters Building and took it to his apartment. Kampiles resigned in October 1977 after receiving a warning letter the previous month for poor performance. He subsequently took the manual to Athens, Greece, where he sold it to a Soviet Embassy official for $3,000. Kampiles was arrested by the FBI in August 1978 and confessed to the theft and sale of the manual to the Soviets. On 22 December 1978, he was sentenced to 40 years in prison.

LESSONS OF CASE/CORRECTIVE ACTIONS

- The Kampiles case illustrated the value of assigning career security officers to line components where they can monitor operational activity closely and spot possible personnel security problems early. Following the Kampiles case, a major drive was launched to place security careerists "in residence" in all the major components of the Agency. This drive is now finished and deemed successful.

- The Kampiles case showed the need for security awareness programs to be aimed at individual employees and at supervisors. After the case broke, a new group was established in the Office of Security for this purpose with additional personnel dedicated exclusively to security indoctrination and security education activity.

- The Kampiles case determined that there was a need to conduct a comprehensive review of new Agency employees early on and certainly before the end of a three-year "probationary period." Subsequent to the case, procedures were established to provide such screening by the Offices of Personnel, Security and Medical Services, along with a performance/suitability assessment by the supervisory chain of command. The review conducted by the Office of Security includes both a reinvestigation update and a polygraph reinterview.

° The Kampiles case led to a conclusion that physical security programming needed to be strengthened. Measures were taken to improve compound perimeter security by upgrading the fences, outdoor lights, alarms, guard consoles, and badge controls. Steps were also taken to upgrade the overall security access system.

° The Kampiles case highlighted concerns over document controls. New emphasis was given to strict accountability for Top Secret and other highly sensitive documents. Disseminations of sensitive intelligence reports were curtailed in strict conformity with the "need-to-know" principle.

° The Kampiles case brought attention to registry operations, policies and procedures. Following a full review of this matter, steps were taken to establish a separate career service for registry officers and information control specialists. Tighter controls were established on the flow of documents and a program for periodic audits of controlled documents was established.

° The Kampiles case illustrated the importance of psychological assessment as a prelude to appointment to sensitive positions. If the individual's self-image and the nature of his assignment are widely discrepant, serious maladjustment may ensue. The Agency has reacted to this possibility by significantly increasing its reliance upon psychological testing prior to employment.

DEPARTMENT OF THE AIR FORCE

PRESENTATION TO
COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

SUBJECT: THE AIR FORCE PERSONNEL SECURITY PROGRAM

STATEMENT OF: DIRECTORATE OF INFORMATION SECURITY
AIR FORCE OFFICE OF SECURITY POLICE
UNITED STATES AIR FORCE

APRIL 16, 1985

NOT FOR PUBLICATION UNTIL RELEASED
BY THE COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

I. OVERVIEW OF THE AIR FORCE PERSONNEL SECURITY PROGRAM.

The Department of the Air Force Personnel Security Program (PSP) is established and administered in accordance with Department of Defense (DOD) Directive and Regulation 5200.2, DOD Personnel Security Program. The Air Force implements DOD Directive and Regulation 5200.2 by Air Force Regulation 205-32.

DOD 5200.2-R/AFR 205-32 state as their purpose: "To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense (DOD), and granting members of the Armed Forces, DOD civilian employees, and other affiliated persons access to classified information are clearly consistent with the interests of national security."

The agency responsible for administering the PSP within Air Force is Headquarters, Air Force Office of Security Police, Directorate of Information Security (HQ AFOSP/SPI), which is located at Kirtland Air Force Base, Albuquerque, New Mexico.

PSP activities include: (1) requesting Personnel Security Investigations (PSIs); (2) evaluating the results of PSIs; (3) granting security clearances; (4) actions to deny a security clearance, to include due process procedures; (5) continuous evaluation of an individual's eligibility to retain a security clearance, to include special investigative inquiries to resolve allegations and revocation of an existing security clearance (with due process); (6) program reviews to determine proper implementation of the PSP; and (7) security education programs. This list is not exhaustive.

Personnel security investigations are required for four primary reasons: (1) to determine suitability for commissioning, enlistment, and civilian employment; (2) as a basis for the granting of a security clearance; (3) to explore and evaluate allegations concerning individuals who possess current security clearances; and (4) periodic reinvestigations.

Suitability requirements: At a minimum, either a National Agency Check (NAC) for commissioning or an Entrance National Agency Check (ENTNAC) for enlistment is required for all Air Force military members. A National Agency Check with written inquiries (NACI) is the minimum investigative requirement for federal civilian employees occupying a nonsensitive or noncritical sensitive position. Either a Background or Special Background Investigation (BI/SBI) is required for the occupant of a critical sensitive position.

Basis for security clearance for US citizens: The minimum investigative requirement for a Secret security clearance concerning a U.S. citizen military member is a NAC or ENTNAC. The minimum investigative requirement for a Secret security clearance for a federal civilian employee is a NACI. The minimum investigative requirement for a Top Secret clearance for a federal civilian or U.S. citizen military member is a BI or SBI. (NOTE: An SBI/Top Secret clearance is required only for some Presidential Support duties, Sensitive Compartmented Information (SCI) access, DOD Courier duties, Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI) access, investigative personnel, and some approved, special access programs. All other Top Secret clearances may be based on a BI.)

Allegations concerning personnel who are presently cleared: A Special Investigative Inquiry (SII) is requested to prove or disprove relevant allegations that have arisen concerning individuals upon whom a personnel security determination has been made previously resulting in a security clearance. An SII is also required to update or assure the completeness of a prior personnel security investigation.

A Periodic Reinvestigation (PR) is required for two basic reasons: (1) to perform an internal review of records concerning Office of Personnel Management (OPM) federal civilians occupying critical sensitive positions for five continuous years (excluding special access programs), and (2) to meet the PR requirements of various security programs in which DOD participates.

Air Force civilian positions are required by Executive Order 10450 to be designated as to "position sensitivity." "Position sensitivity" designations basically reflect the relative damage the incumbent's misconduct, nonfeasance, or malfeasance could cause to national security. The three position sensitivity designations are nonsensitive (no clearance or access required), noncritical sensitive (normally, a Secret security clearance and/or Secret access required), and critical sensitive (normally, a Top Secret clearance and/or Top Secret access required). Military positions are not subject to position sensitivity designations. Security clearance requirements are determined by the location, job, and access requirements where the military member is assigned. One assignment could require an SBI and Top Secret clearance. A subsequent assignment could require only a Secret clearance; however, the individual, once granted a security clearance, continues to be eligible for Top Secret access on a "need to know" basis in the absence of any subsequent unfavorable information.

OPM conducts NACI investigations concerning Air Force federal civilians occupying nonsensitive and noncritical sensitive positions. NAC and ENTNAC investigations concerning military personnel are conducted by the Defense Investigative Service (DIS). DIS conducts both BIs and SBIs concerning military personnel and Air Force federal civilian personnel occupying critical sensitive positions.

All personnel security investigations conducted by DIS, OPM, or any other investigative agency concerning Air Force personnel worldwide are adjudicated by the Air Force central adjudicative authority, the Air Force Security Clearance Office (AFSCO). AFSCO is the sole initial Air Force authority for granting, denying, or revoking security clearances. Appeals of denials and revocations are decided by the Administrative Assistant to the Secretary of the Air Force. All adjudicative actions are performed under the authority of the Secretary of the Air Force.

All personnel security investigations and clearances concerning contractor personnel are under the auspices of DIS. Air Force Intelligence Service and a few other sensitive groups are the access-granting authorities for contractor personnel when Air Force special access or SCI access is involved.

II. THE IMPORTANCE OF PERSONNEL SECURITY.

National security requires that, at a minimum, loyalty and suitability standards be established concerning Air Force personnel.

The personnel security standard applied to determine whether an Air Force person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interest of national security.

The personnel security standard applied to determine whether a person is suitable, under national security criteria, for Air Force appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

The Personnel Security Program is the most logical and efficient means of obtaining information about and evaluating those personal characteristics of an individual which have proven the best indicators of trustworthiness and loyalty. Without personnel security investigations and subsequent evaluation of those investigations, the most objective and accurate means known to us for determining a person's loyalty and trustworthiness would be lost.

III. SPECIFIC ISSUES.

1. Effectiveness of Executive Order 10450: The effectiveness of the Order is diminished because (i) it does not adequately distinguish personnel security requirements from general suitability requirements, and (ii) it does not apply to either military personnel or cleared contractor personnel. These issues are being addressed by an interagency group chartered by NSDD-84; we are confident they will be resolved and that Executive Order 10450 will be replaced with a new Order (or Orders) that will clearly separate personnel security from personnel suitability requirements. Paragraph IV, below, contains an example of a problem resulting from the blurring of personnel security and suitability requirements.

2. Ability to detect from a background investigation potential security violators: We believe the background investigation provides adequate information to identify potential security violators. Our experience is that most security violations are caused by an individual's carelessness, inattention to detail, and/or failure to abide by established rules and regulations. The subject of a personnel security investigation whose history reflects disregard for established rules and regulations would be a prime candidate for a security violation. When a subject's background investigation

reveals a history of gross disregard for established rules and regulations, that individual will likely not receive a security clearance.

3. Continuous assessment of personnel with clearances and access: The Department of Defense and the Air Force have established procedures for the continuous evaluation of eligibility for security clearance and access to classified defense information. Responsibility is placed with Air Force commanders, supervisors, and peer workers to recognize and report incidents and behavior that may have a bearing on an individual's trustworthiness. These procedures do not identify everyone, but they are effective. To further evaluate those individuals who are currently cleared and have access to classified defense information, DOD has implemented a program of Periodic Reinvestigations (PRs). PRs appear to be of great value in detecting changes in an individual's life which may make that individual a security risk. Due to budgetary constraints, this program is currently limited to those having access to our most sensitive programs. History teaches us that most espionage cases involve people who are currently cleared for access and have been cleared for an extended period. Consequently, we believe that periodic reinvestigation is a critical tool for identifying individuals who are potential risks to the national security. The Air Force discerns no identifiable problems with this program.

4. Investigative procedures and techniques: The Air Force is not in a position to identify any problems in this area: the Defense Investigative Service (DIS) and the Office of Personnel Management (OPM) conduct personnel security investigations for all DOD components. Current investigative procedures and techniques appear generally good, except as noted in paragraph IV, question 1, relating to the effectiveness of Executive Order 10450.

5. Adjudicative procedures and techniques: We believe current adjudicative procedures and techniques are objective, impartial, and productive. All personnel security investigations concerning Air Force members are forwarded to AFSCO for adjudication. Personnel security adjudication involves a common sense approach based upon "the whole person" concept in conjunction with formalized adjudicative guidelines. Adjudicative guidelines were developed by DOD and are used by all DOD components in the adjudication of personnel security investigations. AFSCO's adjudicative staff is composed of experienced and trained professionals who objectively apply the standardized adjudicative guidelines and arrive at common sense determinations. Any personal knowledge of the subject as a factor which might bias adjudicative decisions is removed. This process is the best available for determining the suitability, loyalty, and trustworthiness of Air Force personnel.

6. Procedures for denial or revocation of security clearances: The procedures currently employed by the Air Force are reasonable and appropriate in light of the importance of the issue at stake and do not place an undue burden on the adjudicative agency. In conformance with DOD guidelines, the Air Force employs the following procedures in either denying or revoking a security clearance.

After considering all available information, the adjudicator submits the decision in the form of a "Notice of Intent to Deny or Revoke Security Clearance" to a senior manager within AFSCO, namely the respective branch chief. If the branch chief agrees with the decision, after review of the case, he/she signs the notice, which is sent to the commander of the individual's unit of assignment, to be presented in person to the individual.

The notice of intent summarizes the information from the individual's background which led to the intended decision, indicates the sources of that information, and cites the DOD adjudication guideline(s) that provide(s) the basis for considering the background as evidence of unreliability or untrustworthiness. The individual is required to acknowledge receipt of the notice by indorsement and indicate whether he/she will rebut the factual information. The individual is given a reasonable period of time in which to submit his/her response.

If the individual does not rebut, a letter is sent, again via the unit commander, for personal presentation, advising that the revocation or denial is final, and further informing the individual of his/her right to appeal the decision to higher authority. If the individual does rebut, the case is reconsidered by the adjudicator and the final decision is coordinated with supervisors up to the branch chief. If the branch chief concludes the denial or revocation should stand, a letter so advising the individual, for personal presentation by the unit commander, is prepared for signature of the Chief, AFSCO, who reviews the case file and, if he/she approves the action, signs the final action letter. That letter advises the individual that the clearance is denied or revoked, indicates why rebuttal was ineffective, and advises of appeal rights.

Denials or revocations of clearance can be appealed to the Administrative Assistant to the Secretary of the Air Force. To do so, the individual submits any appeal material to AFSCO. If AFSCO's decision on the appeal reaffirms the denial or revocation, the case is presented to a Security Review Panel of three senior Air Staff or Office of the Secretary of the Air Force officials, who review the case file and make an independent, written recommendation to the Administrative Assistant to the Secretary of the Air Force (SAF/AA). SAF/AA then reviews the file and the Security Review Panel's recommendation(s) and issues a final decision to the individual through AFSCO and the unit of assignment.

At any stage of the processing until the case is submitted to SAF/AA, AFSCO can reverse its adverse decision based on receipt of substantive evidence from a legitimate source. In such cases, AFSCO notifies the individual, through the unit of assignment, that the clearance has been granted or restored.

7. Position as to the use of a polygraph: The investigative process makes use of a number of instruments, or tools. These tools include checks of medical, educational, national agencies, law enforcement agencies, credit, criminal, and subversive files, interviews with associates, both business and personal, and most recently, interviews with the subject. No single tool is used in isolation or to the exclusion of the others. Rather, each tool complements the others with a synergistic effect on the whole investigative process. The adjudicative process increases in effectiveness and credibility in proportion to an increase in the relevant information that is known about a subject. While the polygraph neither replaces nor supersedes other data sources, its usage, on a controlled, select basis, adds to the number of tools available in the investigative process. Appropriately employed, with realistic constraints such as those recently published within DOD for the "test" program, it can provide a useful supplement which serves to sharpen the investigative profile of an individual.

8. Position as to psychological evaluation: Psychological evaluations are of proven effectiveness when an individual situation indicates their use

is appropriate to reach an adjudicative decision. We do not think their use for each individual requiring access to classified information, or subjected to a personnel security investigation, is appropriate, because the areas to be evaluated are too broad and general to produce useful results. However, the development and use of a general psychological screening device, such as a written test, would help determine an individual's reliability and trustworthiness in conjunction with a background investigation and would be beneficial. Currently, determination of an individual's psychological reliability depends on second-hand behavorial observations seldom witnessed by mental health professionals. We are unaware of any problems associated with the use of psychological evaluations.

9. Impact of the Merit System Protection Board in personnel security matters: We see the potential for a problem in this area. See paragraph IV below for details.

10. Secret clearances: We think a Secret security clearance, based on a favorably completed and adjudicated investigation, is a valid and cost-effective means of permitting members of the Air Force to have access to information classified up to the Secret level, on a need to know basis, when required in the performance of officially assigned duties. In conjunction with other screening tools used by the Air Force, Secret security clearances are low-cost and effective and are based on a reasonable investigation appropriate to the sensitivity of the information involved. We believe the qualification "in conjunction with other screening tools used by the Air Force" is significant. Without the Air Force program of continuous evaluation of personnel and the prescreening an individual receives prior to entering the

Air Force, our evaluation of a Secret security clearance would be less favorable.

11. Effectiveness of the National Agency Check: The National Agency Check (NAC) accomplishes its objective. The prime reason for an initial NAC or Entrance National Agency Check (ENTNAC) is to assist in determining suitability for commissioning or enlisting individuals in the military service. An additional outcome of a favorable completed NAC/ENTNAC is the granting of a Secret security clearance for a U.S. citizen military member. Considering the relatively large number of individuals who are disqualified for commissioning and enlistment in the Air Force as a result of the NAC/ENTNAC, we think it is very effective. Without a prescreening NAC/ENTNAC, we can project spending a tremendous amount of money for recruiting and training of some individuals who would later be found to be unsuitable for the military service, or worse, could pose a risk to the national security.

12. Government oversight of personnel security of contractors: We think this program accomplishes its mission. The Industrial Personnel Security Clearance Program is administered by the Defense Industrial Security Clearance Office (DISCO) under the policies of the Defense Investigative Service (DIS) and the Office of the Deputy Under Secretary of Defense for Policy (OUSD(P)). Personnel security investigations of contractor employees are conducted by DIS and the resultant security clearances, when appropriate, are granted by DISCO. Compliance inspections to insure that contractors are properly applying industrial personnel security requirements are conducted by the eight DIS Cognizant Security Offices throughout the United States.

13. Ambiguity in dealing with security and suitability matters: We think some ambiguity exists when dealing with security and suitability matters. See paragraph IV for details.

IV. FOR THE ABOVE POINTS, IDENTIFY AND DISCUSS AREAS WHERE THERE ARE DEFICIENCIES AND NOTE EXAMPLES OF PROBLEMS THAT LEND THEMSELVES TO SECURITY RISKS:

1. (Reference paragraph III, question 1). Because of the wording of EO 10450, OPM expands NACIs only to resolve loyalty issues. As a result, we frequently receive completed NACIs with serious issues, such as criminal arrests and drug abuse, unresolved. Failure to reopen such a case could lead to the granting of a clearance when such action is not warranted. We must then request that DIS reopen the case to obtain additional information on which the Air Force can base a determination as to the employee's suitability for employment or eligibility for a security clearance. The reopening of cases under these circumstances reduces the risk to security but adds to the investigative workload, does not properly utilize investigative resources and delays the clearance decision. Current proposals by the NSDD-84 interagency group studying the personnel security program should provide a permanent fix, to include a new Order (or Orders) to replace Executive Order 10450, such Order (or Orders) to clearly separate personnel security from personnel suitability requirements.

2. (Reference paragraph III, question 9). The Merit System Protection Board (MSPB) has recently begun the practice of reviewing the reasons for revocation or denial of a security clearance when the revocation or denial leads to a removal or demotion. We consider this practice potentially damaging to the personnel security program for two reasons. First, we are

opposed to this concept because it impinges on the authority of an agency head to control classified information in his/her custody. That an agency head has this authority is clearly stated in Executive Order 12356, Section 4.1(a): A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials . . . . Second, the MSPB is not experienced in making security determinations nor are they chartered to do so. Because of this lack of experience, there is greater room for error in their judgment with respect to rulings regarding security clearances. In suitability cases, the MSPB's primary area of interest, a ruling in favor of the individual, albeit erroneous, results at worst in the employment of an individual of marginal utility. However, in the area of security clearances, error has an impact on national security: it provides conditions for the inflicting of damage which cannot be undone. Proof and process should be different for the two types of cases; we are concerned that the more lenient standards used by the MSPB for suitability cases will be used in clearance cases brought before them.

3. (Reference paragraph III, question 13). Substantial ambiguity is created by the EO 10450's blurring of security and suitability requirements (refer to paragraph IV, question 1). Some ambiguity is inevitable because behavior relevant to security and suitability covers broad spectra which often--but not always--overlap. It would be beneficial if the criteria for security and suitability were updated and clarified, their commonalities and differences articulated and rationalized. Such guidance would eliminate doubt as to the propriety of certain policies and procedures in our personnel security program and would be the basis for initiatives to enhance it. We believe the product of the NSDD-84 interagency group will give us this guidance.

STATEMENT SUBMITTED BY

COLONEL CHARLES J. LITTLE

U. S. ARMY

CHIEF, OFFICE OF SECURITY

DEFENSE INTELLIGENCE AGENCY (DIA)

BEFORE THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

AT HEARINGS ON

U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM

FEBRUARY 1985

RESPONSE TO INQUIRY FROM THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

I. DIA PERSONNEL SECURITY MISSION

The Director of DIA is one of the five senior officials of the Intelligence Community within the DOD. His authority and reponsibilities encompass management of the Sensitive Compartmented Information (SCI) Program for the DOD. He is the sole determination authority for approval of SCI access eligibility for DIA and the Defense Components (less the National Security Agency). Thus, all requests for SCI access for personnel employed by or assigned to DIA, the Office of the Secretary of Defense, the Organization of the Joint Chiefs of Staff, Defense Communications Agency, Defense Logistics Agency, Defense Mapping Agency, Defense Nuclear Agency, Defense Investigative Service, and Defense Contract Audit Agency are forwarded to the DIA Office of Security for adjudication of access eligibility. The Director's determination authority covers civilian, military, contractor, and consultant personnel who are assigned to the cited components and who require access to any SCI programs or projects. Security clearances (Confidential, Secret, and Top Secret) are granted by the appropriate parent military service or defense component. The Director has, in addition to his SCI mandate, authority to grant such clearances to civilian personnel employed by DIA. In point of fact, however, all DIA employees require SCI access eligibility.

Whenever DIA renders an "adverse" SCI access eligibility determination regarding an individual under the Director's security congnizance, the appeals procedures set forth in Annex B, Director of Central Intelligence Directive 1/14 are administered by the DIA Office of Security. When an adverse action involves personnel assigned to one of the cited Defense components, DIA security officials coordinate each phase of the appeals procedure with the appropriate component security officer.

II. SPECIFIC RESPONSES TO SUBCOMMITTEE INTERROGATORIES:

A. **QUESTION:** Do DIA investigators in effect adjudicate background investigations?

The abbreviated Report of Investigation (ROI) format currently utilized by the Defense Investigative Service (DIS) constitutes de facto field adjudication of personnel history information developed by DIS investigators. While there is little doubt that any type of investigative activity (criminal, counterintelligence, security) requires experienced field agents to exercise "on-the-spot" common sense judgments regarding the nature of the source, the value of the information, etc. Nevertheless, the extreme degree of informational brevity which charcterizes DIS ROI's is, from the adjudicative viewpoint, counterproductive. The bedrock purpose of any personnel security investiation is (and historically has been) to develop the widest range of characterological information about an individual being considered for a sensitive position with the the U. S. Government. In order to properly access an individual's loyalty, trustworthiness, and ability to safeguard critical intelligence material, the security analyst/adjudicator needs extensive information, both favorable and less than favorable, relating to a person's background and conduct. Without detailed information the security analyst cannot formulate a "whole person" assessment which is so vital to the adjuciation of access eligibility.

Over the course of the past 10-15 years there has been a perceptible erosion of investigative purpose. While the causes for this deterioration are complex, one factor stands out: the recurring imbalance between limited investigative resources versus rapid growth in access/clearance requirements. We have arrived at the regretable point where investigative policy, not adjudicative deliberation, dictates what is "doable." From the analytical standpoint, the tail is wagging the dog. Investigators are prone to say adjudicators are "never satisfied" and inevitably want more information. While this claim may be true in isolated instances, most security adjudicators are aware of the limits of reasonable investigative effort. As a point in fact, adjudicators have generally become more reluctant to request the reopening of field investigations to remedy inadequate coverage because of the likelihood that such requests will be denied on "investigative procedure" grounds.

In the final analysis, the security adjudicator is the individual responsible for determining who is loyal and trustworthy. Such a determination is pivotal in maintaining the integrity of our national security. If the critical information flow to security analysts and senior clearance officials is reduced, the viability of the Federal Personnel Security Program will unquestionably be impaired. To base the personnel security system of this country on the premise "no news is good news" is seemingly self-destructive. There are many facets of human activity which may have a direct bearing on security eligibility but are no longer reported in investigative case files because they do not fall within the narrow limitations of "adverse information." The adjudicative prediction of human reliability is an extremely difficult process which, to be fair both to the government and to the individual, must take into deliberation the favorable as well as any unfavorable aspects of a person's life history. No security adjudicator can function competently without a well-rounded "word picture" of the subject of an investigation. It is the job of the security investigator to develop this picture completely but not to assess the ulitmate value of the print.

B. QUESTION: Impact of monthly quotas on background investigations.

At the present time a quota system constrains the Periodic Reinvestigation (PR) program, but not the intiial background investigation program. Under the provisions of the Director of Central Intelligence policy, every individual who is cleared for access to Sensitive Compartmented Information (SCI) must be reinvestigated on a five-year basis. In 1981, the Deputy Security of Defense, responding to severe manpower decrements in the Defense Investigative Service (DIS), mandated a moratorium on 5-year update investigations. This moratorium was lifted in 1983 to the extent that a monthly PR case submission quota was imposed on all DOD elements. Unfortunately, the two-year moratorium created a backlog of outdated security files. The follow-on quota system inhibits the ability of security authorities to maintain current assessments of cleared personnel in accordance with DCI policy. The effect of a quota backlog on the security vulnerability of DIA is difficult to assess. Until such time as the Deputy Under Secretary of Defense for Policy lifts the PR quota, Defense agencies and military departments will have to live with a degree of increased security risk.

C. **QUESTION:** Is it prudent for DIA to grant SCI access without polygraph examination?

The DIA, along with the Central Intelligence Agency (CIA) and the National Security Agency (NSA), is one of the major intelligence producers for the U. S. Government. Both the CIA and NSA make extensive use of the polygraph in screening their personnel for access to SCI. In view of the fact that DIA, CIA, and NSA are inexorably interwoven in the exchange of real-time intelligence data, it does not appear logical that DIA should not likewise screen its personnel. Employment with DIA is synonymous with SCI access. Unlike the military services and other Defense agencies, DIA cannot internally transfer an employee who is ineligible for SCI access to less sensitive, non-SCI duties. There have been frequent instances over the years where fully-cleared DIA employees who were nominated for joint Intelligence Community assignments were unable to successfully complete a required pre-assignment polygraph examination. In almost all such cases, subsequent additional field investigation by DIA and/or the Defense Investigative Service resulted in dismissial from DIA employment.

Recent Congressioal action permits DIA to polygraph, on a provisional basis, a restricted number of employees who occupy "critical intelligence positions." Although DIA views this authority as a step forward, recent espionage history suggests that hostile intelligence services expend considerable effort in attempts to recruit fully cleared personnel who have extensive classified access but who occupy lower paying positions. Such individuals (often administrative personnel) would not necessarily be included in a definition of "critical intelligence" duties.

D. **QUESTION:** How does DIA adjudicate emigre cases?

DIA does not clear non-U.S. citizens. Naturalized United States citizens are subject to the same investigative criteria as native-born citizens; however, the lack of polygraph authority to verify a foreign-born person's life history prior to entry into the United States restricts our ability to employ such individuals.

E. **QUESTION:** Provide an assessment of the continuing hostile intelligence threat to NATO operations.

Since the signing of the North Atlantic Treaty on April 4, 1949, the North Atlantic Treaty Organization (NATO) has been perceived by the Soviet Union and its European allies as a continuing threat to East European security. In the intervening years the Warsaw Pack has mounted a significant intelligence collection effort directed against participating members of the NATO alliance.

Counterintelligence efforts of the Western European member nations have resulted in the revelation of large numbers of hostile human intelligence (HUMINT) operations directed against NATO since the earliest days of its formation.

Numbers of successful hostile penetrations of NATO personnel with access to classified information does not in itself fully address the problem. Of the numerous cases which have come to public attention, a high percentage have involved individuals who have successfully performed espionage on behalf of the Warsaw Pack for five, ten, fifteen years, and even longer. Cases have been revealed in which literally thousands of classified NATO documents were passed by the collaborator to his or her Warsaw Pack contact. By comparison, very few Americans have been known to operate successfully as espionage agents for hostile intelligence for periods longer than one or two years. Additionally, there have been numerous cases in which a NATO member nation has declared officials of the Warsaw Pack to be persona non grata (PNG) for activities incompatible with their status. Frequently, the host government has publicly offered no concrete rationale for the PNG action. The April 1983 PNG action by France, in which 47 Soviet officials were asked to leave the country, is an example of French reaction to what may have been extensive espionage activity by the Soviets in France. Of major concern to the United States is the continuing problem of technology transfer via West European conduits, to include those technologies which are obtained through clandestine as well as open or "gray" means, which impacts on the technology edge held by the United States and its allies.

The conduct of intelligence operations in Western Europe by the Warsaw Pack is facilitated by common borders and common heritage and by its relatively permissive society. Sentencing of convicted agents in Western Europe rarely results in prison sentences of more than a few years. A recent notable exception was the conviction of Geoffrey Arthur Prime, a British citizen who provided communications information to the Soviets for almost 20 years. His conviction resultd in a sentence of 35 years in prison.

As long as NATO is perceived to be a threat and a lucrative area for espionage, the Warsaw Pack will continue (and probably escalate) their intelligence collection efforts targeted against NATO.

UNITED STATES GOVERNMENT
# memorandum

DATE: 3 December 1984

REPLY TO ATTN OF: DI-3 U-709/DI-3

SUBJECT: Espionage Directed Against the United States

TO: Senate Committee on Governmental Affairs
Permanent Subcommitte on Investigations

1. In response to your request for information, enclosed is an unclassified summary of significant espionage cases involving individuals who have been convicted of compromising U.S. classified information.

2. These case studies involve compromise of DoD and DoD-related classified information and were compiled solely from publicly available open sources. DIA's limited purpose in retaining such information is in connection with the Counterintelligence Division's functional responsibility to analyze and produce information on the hostile human intelligence threat to DoD. DIA is not and should not be viewed as a reference service, clearing house, or coordinating agency for espionage cases or espionage information.

3. DIA provides the enclosed, cognizant of and in compliance with, the Privacy Act of 1974, as amended (5 U.S.C. 522a) and DoD Regulation 5240.1R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," 7 December 1982.

Kenneth E. Geisen
KENNETH E. GEISEN
Chief, Legislative and Public Affairs
Division (DI-3)

OPTIONAL FORM NO. 10
(REV. 1-80)
GSA FPMR (41 CFR) 101-11.6
5010-114

* U.S. GOVERNMENT PRINTING OFFICE : 1982 O - 361-526 (8017)

William KAMPILES - KAMPILES is an egocentric individual who was the only child of a doting mother whose husband died when William was young. Recruited for the CIA on his college campus, KAMPILES wanted to be a spy in CIA's Directorate of Operations. His initial assignment to CIA's Watch Center was boring to KAMPILES and both his work and his associations at the Agency bordered on unsatisfactory. His work performance resulted in the rejection of his requests for a transfer to operations and, in less than one year following his hire, KAMPILES resigned from the Agency. Prior to his resignation, KAMPILES took from the Watch Center a TOP SECRET manual which gave the precise workings of the KH-11 reconnaissance satellite. Shortly following his resignation, KAMPILES took this document to the Soviet Embassy in Athens where he offered the manual for $10,000. Several days later the Soviets provided KAMPILES with $3,000 and attempted to persuade him to rejoin the CIA. KAMPILES' role in providing the Soviets with the KH-11 manual was soon discovered, resulting in his trial and conviction on charges of espionage. The principal motivating factors in this case were ego and disgruntlement.

William Holden BELL - The June 1981 arrest of William Holden BELL is a classic example of hostile expionage. Not a volunteer for espionage, BELL had been carefully assessed, cultivated, and recruited into the role of spy. Having lost a son to whom he was very close, gone through a divorce and remarriage, and faced with mounting debts, BELL was ripe for recruitment. By chance BELL met a neighbor, Marian Zacharski, who was a representative for the Polish import-export company, Polamco. Over ensuing months Zacharski, who used Polamco as a cover for his intelligence activity, cleverly cultivated BELL to a point that BELL became relatively dependent on Zacharski for his companionship, the interest Zacharski displayed in BELL's welfare, and hints of possible mutual business opportunities. This closeness eventually resulted in BELL providing Zacharski with both classified and unclassified documents from his place of employment, the Hughes Aircraft Company. BELL had been paid $4,000 by Zacharski for having provided some names as possible contacts for Polamco machinery sales. The stage had been set for a successful recruitment of BELL. By chance the apartment complex in which the two families were living was being converted to condominiums and BELL did not have the down payment required for purchase. Expressing his disappointment to Zacharski over the matter, Zacharski suggested that Polamco might be able to help. Shortly thereafter, in two separate payments, Zacharski provided a grateful BELL with a total of $12,000. Soon BELL began to provide favors to Zacharski and from 1979 to 1981 BELL turned over Hughes documents dealing with material to include: the F-15 look-down-shoot-down radar systems; the quiet radar system; an all-weather radar system for tanks; an experimental radar system for the U.S. Navy; the Phoenix air-to-air missile; a shipborne surveillance radar; the Patriot surface-to-air missile and a NATO air defense system. An extremely effective, albeit young, hostile intelligence officer combined fortuitous circumstance with assessed monetary need and ego, to recruit a U.S. citizen for espionage resulting in serious compromise of U.S. military radar and defense systems.

David Henry BARNETT - BARNETT had worked as a contract employee and later as a regular employee of the CIA from 1958 until 1970 when he resigned to establish a private business. In 1976, with a failing business and mounting debts, BARNETT offered to reveal to the KGB his knowledge of CIA activities. Initially asking $70,000 for his information, BARNETT provided the names of CIA agents and officers known to him for which he was paid $25,000. In 1977 BARNETT revealed to his Soviet handlers all he knew concerning CIA operations including the reason why Soviet SAM-2 missiles had been largely unsuccessful in hitting the B-52 bombers flying over Vietnam. He also revealed information on KGB officers whom the CIA had identified as being possibly susceptible to a U.S. recruitment attempt. The Soviets saw that since his information, while valuable, was somewhat dated he would be of more value if he were to rejoin the CIA. He was therefore instructed to attempt to obtain a position with the CIA, Bureau of Intelligence and Research at the State Department, DIA, the White House Intelligence Oversight Board, or the Senate or House Intelligence Committee. He was re-hired by the CIA in 1979 as a contract employee to teach classes on resisting interrogation. He continued cooperating with the KGB until March 1980 when confronted by the FBI after their interception of communications between BARNETT and his KGB handlers. This case demonstrates that serious financial problems can cause an individual to take extreme measures with apparent little or no forethought as to the consequences of the action to national security.

Philip AGEE - Although not an espionage agent in the classic sense, AGEE nevertheless damaged his country as a result of his personality weaknesses and disgruntlement. Having been forced to resign from the CIA for improper behavior and financial problems, AGEE turned to Cuban and Soviet intelligence as a result of his bitterness. His cooperation with the DGI and KGB was followed by his embracing of Communism and strong declaration of anti-U.S. sentiments.

Walter SPAWR - A non-DoD case with potentially far-reaching military implications, SPAWR conspired to sell embargoed technology to the Soviets. The technology, highly polished laser mirrors, was a technological process discovered by SPAWR himself. Following illegal diversion of a total of 30 of these mirrors to the Soviet Union, SPAWR was offered $1.5 million to sell his techniques to the Soviets and to teach them the process of producing the mirrors. The FBI learned of these exports and in 1980 SPAWR and his wife were convicted on 11 charges of conspiracy, submission of false statements to the government, and illegal exportation of laser mirrors to the Soviet Union.

Robert Lee JOHNSON - In the fall of 1952 Sergeant Robert Lee JOHNSON was a disgruntled soldier stationed in Berlin. Having been passed over for promotion and carrying other grievances against the U.S. Army, JOHNSON decided that he would defect to the Soviet Union and enlisted the aid of his mistress to make initial contact with the Soviets in East Berlin. In February 1953 a meeting was established and two KGB officers questioned JOHNSON extensively. Having determined that JOHNSON was intent on "getting even" with the Army for his perceived mistreatment, the Soviets convinced him to remain on duty while acting as an agent of Soviet intelligence. At the time JOHNSON did not appear to the Soviets to be of any immediate use but they were willing to gamble on his future potential. Subsequent events reflected the foresight of the Soviets in continuing to cultivate JOHNSON. Two months later JOHNSON married his mistress and both individuals were given intelligence training by the Soviets who even arranged for a psychiatrist to interview JOHNSON. As one of his first tasks, JOHNSON arranged a transfer to the office of the G-2, Berlin Command, as a clerk. At about that time a close friend of JOHNSON's, Sergeant James Allen MINTKENBAUGH, arrived in Berlin on assignment. In short order JOHNSON "recruited" MINTKENBAUGH into helping him provide information to the Soviets. MINTKENBAUGH was a homosexual and this fact interested the KGB handlers since the homosexual frequently is shunted by society and made to feel like a social outcast. Such a personality may seek to retaliate against a society that has placed him in this unenviable position. MINTKENBAUGH was such a person and one of his first assignments on behalf of Soviet intelligence was to spot other homosexuals in the American community. During the first three years as a Soviet agent JOHNSON apparently provided little information of real value and in 1956 accepted a discharge from the Army. Not successful in civilian life, JOHNSON was ripe for returning to the military when MINTKENBAUGH appeared at his door with $500 from his former Soviet handler. MINTKENBAUGH was still involved with the KGB who proposed that JOHNSON return to the service and attempt to obtain information on U.S. missiles. Unable to enlist in the Air Force, JOHNSON returned to the Army and was stationed at a Nike-Hercules missile site. In that assignment he was able to provide photographs and diagrams of the Nike-Hercules and information about its characteristics. Additionally he was successful in siphoning off a sample of the rocket fuel. This assignment was followed by a tour at Fort Bliss where JOHNSON continued to provide missile data and other classified information. In the interim MINTKENBAUGH was escorted to Moscow where he was tasked to marry a Soviet illegal and open a business in Washington, D.C. Before that, however, he was to make contact with JOHNSON who had been transferred from Ft. Bliss to Orleans, France. JOHNSON was instructed to attempt to obtain a position at SHAPE, then in Paris, since he had no access in his position in Orleans. JOHNSON was unsuccessful in obtaining a SHAPE assignment but in casual conversation with a fellow soldier he learned about the possibility of being assigned to the Armed Forces Courier Center at Orly Air Field near Paris. The Courier Center was a trans-shipment point for highly sensitive and classified documents, cipher systems, and cryptographic equipment destined for points within NATO, the European Command and the Sixth Fleet. Although in-depth security measures were employed at the courier station, circumstances again played a role and JOHNSON eventually was able arrange for his transfer to Orly where he eventually was able to gain access to the vaulted material. Once access had been achieved the Soviets devised an elaborate means of removing and photographing the documents and then returning the material to the pouches leaving no trace of their having been opened. JOHNSON would return the pouches to the vault with no one ever knowing that the material contained therein had been compromised. The damage done by JOHNSON's pilfering of the Courier Center vault has been characterized as "enormous." He was eventually reassigned to Washington where he once again saw MINTKENBAUGH. MINTKENBAUGH related that he had lived for six weeks in Canada collecting documents to be used by Soviet illegals for infiltrating into the U.S. and had, as a real-estate salesman, also provided personalia on government employees who were seeking housing in the Washington area. Not long thereafter JOHNSON deserted the Army and wandered aimlessly for a month until turning himself in to authorities. JOHNSON's wife, in the meantime, had confessed to their espionage activities to include those of MINTKENBAUGH. Both men fully confessed to the roles they played on behalf of the KGB and both indicated that their motives had been revenge, JOHNSON wanting to "get back" at the Army and MINTKENBAUGH feeling that he was one of God's mistakes who should have died as a baby. JOHNSON had no way of identifying the information compromised in Paris but damage was extremely serious and long-lasting.

William Henry WHALEN - Arrested in 1966, retired U.S. Army LTC WHALEN's terminal assignment was to the Office of the Joint Chiefs of Staff. He was sentenced to fifteen years imprisonment for espionage conducted on behalf of the Soviets. WHALEN was paid over $3,000 for his espionage activity between December 1959 and December 1961.

Walter T. PERKINS - Sergeant PERKINS was a member of the U.S. Air Force assigned to the Intelligence Section, Air Defense Weapons Center, Tyndall Air Force Base, Florida. PERKINS was apprehended in October 1971 with classified documents intended for passage to a Soviet KGB officer in Mexico. He had access to TOP SECRET documents dealing with plans for combating Soviet air attack.

James D. WOOD - Arrested by the FBI on 2[illegible] July 1973, US Air Force Sergeant James D. WOOD was in possession of classified counterintelligence information intended for passage to a first secretary of the Soviet Embassy.

Christopher M. COOKE - COOKE was a 2nd Lieutenant in the U.S. Air Force and Deputy Commander of a Titan missile crew at McConnell Air Force Base near Wichita, Kansas. He allegedly made several visits to the Soviet Embassy in Washington, D.C. where he turned over classified nuclear information. Due to procedural irregularities, COOKE was not tried although he was discharged from the service. In his confession, which was allegedly given on condition of full immunity, COOKE admitted to turning over nuclear secrets and that he had been attempting to entice the Soviets in using him as a "...medium for the promulgation of a policy shift or some sort of initiative which would provide me with a first-rate piece of publishable material." The extent of his activities and his true motives will probably never be known; however the Air Force was sufficiently concerned that they changed the codes used for sending launch messages and they retargeted some of the missiles. All indicators point to the likelihood that COOKE voluntarily entered the Soviet Embassy and had not been sought out by their intelligence apparatus.

Jack Edward DUNLAP - Sergeant DUNLAP sold classified documents from NSA to the Soviets for four years (mid-59 to mid-63) for which he was paid approximately $60,000. DUNLAP was first a driver and then a clerk-messenger at NSA when he was contacted by the Soviets and agreed to work for them. It was only following DUNLAP's suicide that his wife discovered classified documents secreted in their home. The extent of his espionage activity cannot be accurately determined but it is apparent that his primary motivation was monetary.

William Hamilton MARTIN and Bernon Ferguson MITCHELL - These two friends worked at the National Security Agency (NSA) for three years when they defected to the Soviet Union. On 6 September 1960 they held a press conference in Moscow at which they revealed, among other things, that NSA had broken the codes of more than half of the nations which encoded message traffic. They stated that they defected due to their dissatisfaction over some of the practices of the United States in its intelligence gathering activities. They also lauded the USSR for its practice of encouraging the talents of women. Both men were described as being bright and both were quite knowledgeable of NSA activities and personnel. It must be assumed that they willingly told the Soviets everything they knew following their arrival in Moscow.

Roy Adair RHODES - Master Sergeant RHODES was one of the first Americans to be recruited by Soviet intelligence following World War II. He was also one of the few Americans known to be blackmailed into espionage. Sergeant RHODES was in charge of the motor pool at the U.S. Embassy in Moscow in 1952. He had gone there without his wife and child and, following a drunken party, he was photographed in bed with a Soviet woman. The subsequent threat of exposure resulted in RHODES' agreement to cooperate with Soviet intelligence. Following his transfer to the United States in 1953 he had no further contact with the Soviets even though they searched for him in an attempt to continue the clandestine relationship. RHODES was not of great value to the Soviets at the motor pool; however they had plans for him to take training as a mechanic on code machines. Ultimate damage in this case was minimal although there was great potential for significant and long-lasting compromises.

James Durward HARPER, JR. - On 15 October 1983 a freelance computer engineer, James Durward HARPER, Jr., was arrested and charged with receiving $250,000 for providing classified U.S. documents to Polish intelligence. HARPER, 49 years of age at the time of his arrest, had obtained information concerning U.S. missile defenses from his wife Ruby Louise Schuler Harper. Mrs. Harper was employed as an executive secretary for Systems Control Inc. where she had access to numerous classified and unclassified documents concerning the Minuteman and other Intercontinental Ballistic Missiles (ICBMs). HARPER had initially contacted Polish intelligence in 1975 through an introduction by William Bell Hugle. Hugle was cut out of the picture by Polish intelligence and HARPER continued to provide classified information to the Polish intelligence service. The information was considered so valuable that the Poles invited the Soviets to bring in teams of experts to Warsaw to examine the documents. On 12 December 1983 HARPER pleaded not guilty to charges of stealing U.S. missile secrets and selling them to Poland. He was charged on nine counts of espionage and tax evasion, and accused of illegally obtaining 61 classified documents of which 21 were sold to the Poles. At the 14 May 1984 sentencing of HARPER the Prosecution stated that the Government found HARPER to be a sociopath with no sense of honor or morality. The Judge found that at no time did Harper say he was sorry, shameful or regretful for his actions; that he was a traitor for greed and money. The Court found that HARPER's actions had exposed all U.S. citizens to risk and danger, a danger that could well extend into the 21st century. HARPER was sentenced to life in prison.

Nelson Cornelious DRUMMOND - U.S. Navy Yeoman Nelson Cornelious DRUMMOND was recruited by Soviet intelligence while on assignment in London in 1957. He was arrested in September 1962 on charges of providing U.S. Navy classified information to the Soviet Union. Although DRUMMOND insisted that many of the documents he passed had been declassified, the court considered the damage so serious that DRUMMOND was given a sentence of life in prison. It was reported that $200 million had to be spent on countermeasures as a result of DRUMMOND's espionage activity. He reportedly received between $20,000 and $24,000 for the information passed; his apparent motivation was monetary.

Waldo H. DUBBERSTEIN - On 28 April 1983 Waldo H. DUBBERSTEIN was indicted by a federal grand jury on charges of selling U.S. military secrets to Libya. The following day the 75-year old DUBBERSTEIN was found dead, his death later being ruled a suicide. DUBBERSTEIN had served for 24 years with the CIA and 11 years with DIA, retiring from DIA in 1982. The seven count indictment against DUBBERSTEIN charged him with conspiracy, making a false statement about travel abroad, three counts of unauthorized disclosure of classified material, one count of bribery and one count of illegal gratuity. Had DUBBERSTEIN been convicted he faced a possible sentence of 57 years in prison and $80,000 in fines. DUBBERSTEIN had apparently begun his cooperation with Libya as an outgrowth of his meetings with Edwin P. WILSON who acted as a middleman for passage of information to Libya and receipt of payments from Libya.

Brian P. HORTON - This 28 year old Intelligence Specialist Second Class, U.S Navy, was sentenced on 12 January 1983 to six years in prison for failing to report contacts with the Soviet Embassy in Washington, D.C. and for trying to sell classified information to the Soviet Embassy. Between April and October 1982 HORTON wrote one letter and made four telephone calls to the Soviet Embassy with an offer to provide information on the Single Integrated Operations Plan (SIOP), a classified master plan of how the U.S. would fight a war. No classified information was exchanged and HORTON received no money from the Soviets. His defense attorney argued that HORTON was working on a novel and approached the Soviets to learn their *modus operandi* while the prosecution stated that HORTON had attempted to get between $1,000 and $3,000 for his information.

Stephen BABA - Ensign Stephen BABA was sentenced on 20 January 1982 to eight years at hard labor for sending classified electronic warfare documents to the South African Embassy, Washington, D.C. from his frigate in San Diego, California. In court testimony it was asserted that BABA had supplied the documents to raise enough money to bring a Filipino woman to the United States.

Edwin P. WILSON - Edwin P. WILSON is serving a 32-year prison sentence having been found guilty on charges of arms and explosives smuggling growing out of his Libyan dealings between 1976 and 1982. WILSON also played a role in the DUBBERSTEIN case, having acted as middle man in the passage of information to Libya and making payments to DUBBERSTEIN on behalf of Libyan intelligence.

John William BUTENKO - A civilian electronics engineer, John William BUTENKO was convicted on 2 December 1964 of conspiring to give command and control systems secrets of the U.S. Strategic Air Command to the Soviet Union. BUTENKO had testified that he had met his Russian contacts only because they had promised to give him information about his relatives behind the Iron Curtain. He was given a 30-year sentence.

Joseph P. KAUFFMAN - U.S. Air Force Captain Joseph P. KAUFFMAN was convicted by court-martial in Weisbaden, West Germany, on 17 April 1962, for having passed military secrets to East Germany. A veteran of 19 years of military service, KAUFFMAN was sentenced to 20 years at hard labor.

Joseph George HELMICH - Former U.S. Army cryptographer Joseph George HELMICH was indicted on 15 July 1981 by a federal grand jury on charges of supplying the Soviet Union with coding secrets and equipment. He was specifically charged with delivering TOP SECRET information about the KL-7 cryptographic system to Soviet agents while stationed in Paris in 1963 and 1964. He was also charged with receiving $131,000 from the Soviets in return for the information provided, HELMICH was sentenced to life in prison.

Eugene Lee MADSEN - Yeoman Third Class MADSEN was a 24-year old service member assigned to the Strategic Warning Staff in the Pentagon when he offered to sell classified documents concerning international drug trafficking to an acquaintance. The offer was reported to the FBI who arranged for an undercover agent to receive the documents. Unable to locate the documents on drug trafficking, MADSEN carried out from his work site seven TOP SECRET documents dealing with intelligence assessments of the Near East and South Asia and interpretations of secret photographs. MADSEN was arrested when he turned the documents over to the FBI agent and subsequently pleaded guilty to a single count of espionage. He was sentenced to eight years in prison. MADSEN's professed homosexuality apparently did not contribute directly to his involvement in passing of classified documents; that is, he was not being blackmailed in that he had volunteered to pass the documents. His roommate stated that MADSEN needed money and intended to sell the documents to buy a new automobile.

Victor Norris HAMILTON - On 22 July 1963 Izvestia reported that Victor Norris HAMILTON, a former NSA employee, had asked for political asylum in the Soviet Union. HAMILTON allegedly published a letter charging NSA with intercepting and decoding secret instructions from Arab countries to their UN delegations. Also on 22 July the Department of Defense announced that HAMILTON, a research analyst, had been discharged from NSA for psychiatric reasons in 1959.

Kurt L. PONGER and Otto VERBER - Brothers-in-law Kurt L. PONGER and Otto VERBER were naturalized U.S. citizens who served in the U.S. Army in Europe during World War II. Following their discharge they remained in Germany under civilian employment connected with the Nuremberg war crimes trials. Having been recruited as agents by the Soviets, PONGER and VERBER were instructed to secure information on U.S. installations and personalities. On 8 June 1953 VERBER was sentenced to serve 3 and one third years to ten years and PONGER was given a five to 15 year sentence.

George H. FRENCH - Captain George H. FRENCH, USAF, was sentenced to life imprisonment at a secret court martial on 20 September 1957. He was charged with attempting to sell nuclear bomb information to the Soviet Embassy in Washington, D.C. He was arrested in New York after FBI agents retrieved a letter he had tossed onto the Soviet Embassy premises on 5 April. The letter offered to sell, for $27,500, information he possessed on nuclear bombs and equipment for handling them in B-36s. He was motivated by money and his wife attributed his actions to desperation over $8,000 in poker debts.

Joseph Sydney PETERSON, JR. - A former NSA analyst, Joseph Sydney PETERSON, Jr., was given a seven year prison sentence on his plea of guilty to misusing secret government data. The forty year old PETERSON was arrested on 9 October 1954 having worked for NSA or its predecessors since 1941. PETERSON had been providing information to a Dutch friend about the U.S. breaking of Dutch codes. On 19 October The Netherlands Embassy announced that it had exchanged "secret intelligence" with PETERSON during and after World War II on the assumption that his superiors had authorized the exchange.

Giuseppe CASCIO - Staff Sergeant Giuseppe CASCIO, USAF, was convicted by court martial in Taegu, Korea on 8 June 1953, of conspiring to give jet plane secrets to the Communists. The 34-year old CASCIO was arrested on 21 September 1952 along with Staff Sergeant John P. JONES, USAF, when attempting to pass secret data on the then new model F-86E Sabre jet plane. He was charged with 16 counts of accepting Military Payment Certificates from a Korean civilian. JONES, who allegedly gave CASCIO the data for passage, was judged insane and returned to the United States with no charges being filed. CASCIO was given a 20-year prison sentence.

NAME	RANK/POSITION	DATES OF ACTIVITY	HOSTILE SERVICE	MOTIVATION	MATERIAL COMPROMISED	VOLUNTEERED (V) OR RECRUITED (R)
Jack Edward DUNLAP	Sergeant, US Army Assigned to NSA	mid-1959-July 1963	SIS	Money	Highly sensitive NSA documents	R
Victor Norris HAMILTON (previously HINDALI)	Civilian employee NSA	July 1963	SIS	Ideology	Classified NSA documents on code-breaking in the Near East	V
James Durward HARPER, JR.	Civilian engineer (acquired classified data thru wife)	1975-1983	Polish Intelligence Service	Money	MX/Minuteman missile; U.S. nuclear defense capabilities	R
Edwin G. MOORE, II	Civilian employee CIA	December 1976	SIS	Money	Threw classified CIA documents into Soviet compound; turned over to U.S. authorities as possible bomb; probably no compromise	V
Walter T. PERKINS	Master Sergeant USAF; Intel Section, Air Defense Weapons Center	October 1971	SIS		Had access to U.S. air defense plans	R
Roy Adair RHODES	Master Sergeant Motor Pool, U.S. Embassy, Moscow	January 1952-June 1953	SIS	Blackmail	Apparently passed very little information and that of minimal value	R
Robert Glenn THOMPSON	Airman First Class USAF	June 1957-July 1963	SIS	Disgruntlement(?) Blackmail(?) Money(?)	Classified documents; photos of military equipment, data on missile sites, intelligence information. (THOMPSON frequently changed his story about motivations, activities etc. He allegedly defected to East Germany where the Soviets convinced him to return to his unit and work as their agent)	V/R
William Henry WHALEN	Lt Col (retired) US Army	December 1959-December 1961	SIS	Money	Classified and unclassified U.S. military publications	R

NAME	RANK/POSITION	DATES OF ACTIVITY	HOSTILE SERVICE	MOTIVATION	MATERIAL COMPROMISED	VOLUNTEERED (V) OR RECRUITED (R)
George P. FRENCH	Captain, USAF	1957				
Waldo DUBBERSTEIN	Civilian employee, DIA	1977-1980				
J. PETERS	Illegal Hungarian resident in U.S.	1949	SIS			
James D WOOD	Sergeant, USAF	July 1973	SIS		Classified counterintelligence information	
Brian Patrick HORTON	Intelligence Specialist 2nd Class, US Navy	June-August 1982				
ATTARDI	Staff Sergeant	@1970				TOP SECRET plans from document section Heidleberg
Joseph Sidney PETERSON	PFC(?) NSA cryptologist	1954	Dutch	Naivity(?)	U.S. breaking of Dutch codes	V(?)
Leonard Jenkins SAFFORD	Sergeant, US Army	1964-1967				
William WEISBAND	Armed Forces Security Agency	@1948	Soviet		Revealed to Soviets that US had broken Soviet Code	

NAME	RANK/POSITION	DATES OF ACTIVITY	HOSTILE SERVICE	MOTIVATION	MATERIAL COMPROMISED	VOLUNTEERED (V) OR RECRUITED (R)
Joseph G. HELMICH	Warrant Officer US Army	January 1963- late 1964(?)	GRU	Money	KL-11 crypto material/associated information	V
Christopher M. COOKE	2nd Lt, USAF	December 1980- May 1981	SIS	Ego(?) Research material(?)	Missile codes/nuclear secrets(?)	V
Stephan Antnony BABA	Ensign, US Navy	1982	South Africa		Secret electronics documents	V(?)
David Henry BARNETT	Covert agent CIA	1976-March 1980	KGB	Money	Information on secret CIA operations	V
William Holden BELL	Radar project Engineer, Hughes Aircraft Co.	January 1978- June 1981	Polish Intelligence Service	Money Ego Naivity	Quiet radar; look-down/shoot down radar; other radar; sonar missile systems	R
Christopher John BOYCE Andrew Dalton LEE	Employee TRW	April 1975- 16 January 1977	SIS	Money	Technical data on Rhyolite and Argus satellites	V
John William BUTENKO	Production engineer RCA	21 April 1963- 29 October 1963	KGB	Russian heritage(?)	Data processing, data display programming	R
Raymond George DECHAMPLAIN	Master Sergeant USAF	1971-1975	SIS		Classified military documents	
Sahag K. DEDEYAN	Employee, Johns Hopkins Applied Physics Laboratory	June 1975	SIS		National defense documents to include "Vulnerability Analysis; U.S. Reinforcement of NATO"	V
Nelson Cornelious DRUMMOND	Yeoman First Class U.S. Navy	1957-1964	SIS		Navy secrets	
Ronald Louis HUMPHREY (provided information to David TRUONG)	Civilian employee U.S. Information Agency	January 1978	Vietnam	Hostage (was trying to get mistress out of Vietnam)	Information dealing with U.S.-Vietnamese relations	R

NAME	RANK/POSITION	DATES OF ACTIVITY	HOSTILE SERVICE	MOTIVATION	MATERIAL COMPROMISED	VOLUNTEERED (V) OR RECRUITED (R)
Robert Lee JOHNSON James Allen MINTKENBAUGH	Sergeant, U.S. Army	February 1953-1964	KGB	[illegible]ntlement	Various classified documents from his assignment in Berlin and the U.S. but most damage done by his taking information from courier pouches at Orly Air Field, Paris, while assigned there as guard.	V
William Peter KAMPILES	Watch Officer, CIA	2 March 1978	SIS	Disgruntlement/ Ego	KH-11 manual; blank CIA ID Card	V
Joseph Patrick KAUFFMAN	Captain, USAF	1960		Blackmail	USAF installations in Japan and Greenland; personalia on fellow officers	R
Lee Eugene MADSEN	Yeoman, U.S. Navy	July 1979	Intended to pass info to underworld for onward passage to SIS	Ego(?) Money(?)	Took out classified documents from Watch Center but FBI had been alerted and FBI agent received the information intended for sale	V
Francisco de Asis MIRA	Sergeant, USAF Computer Specialist 601st Tactical Control Wing, Sembach Air Base	May 1982-March 1983	Suspected EGIS or SIS	Dissatisfaction Money Wanted to be double agent	U.S. code books and radar systems reports; maintenance schedules for Air Defense Radar Installations in FRG	V
Philip AGEE	Former CIA Employee		Cuban Intelligence Service and KGB	Disgruntlement		
Walter SPAWR	Private businessman			Monetary	Laser mirrors illegally shipped to USSR	V
William Hamilton MARTIN Bernon Ferguson MITCHELL	Civilian employees NSA	1960	Defected to USSR	Dissatisfaction	Unknown. Possibly everything to which they had access. Both were described as being very bright	V

NAME	RANK/POSITION	DATES OF ACTIVITY	HOSTILE SERVICE	MOTIVATION	MATERIAL COMPROMISED	VOLUNTEERED (V) OR RECRUITED (R)
Ulysses L. HARRIS	Sergeant, US Army	1967				
G. J. GESSNER	Officer, US Army intelligence	Defected 1962			Nuclear secrets	
Glen ROHRER	Warrant Officer US Army	Defected 1964			Polygraph information	
F. BAUER R. HIRT	Sergeant	1945				
M. J. and P. KEENEY	Civilians	1949				
J. P. JONES P. CASCIO	Staff Sergeant	1952				
A. H. COLEMAN	Officer USMC	1953				
G. and J. ZLATOVSKI	J. worked for U.S. Army, Austria	1957 1947-1948	SIS		Photographs and biographics of CIC and CIA officers in Austria; their agents and cons	
E. NELSON		1950				
Leslie J. PAYNE	Specialist 5th Class US Army	1975	EGIS (?)		Classified documents	
Herbert W. BOECKENHAUPT	Staff Sergeant US Army	1966	SIS	Blackmail (threat to father in FRG)		
Kurt L. PONGER/ Otto VERBER	US Army enlisted/ then civilian	1953	SIS		US troop dispositions in Germany/US personalities	R
Two individuals unnamed	High ranking USAF officer; civilian	1953-1954	SIS	Sex (the two men were "used" by Irmgard Margarethe SCHMIDT)	Personal data and duties of the two US officials involved; info on US OB Section, Berlin	

Summary of Significant Cases of Espionage Involving Compromise of NATO-Classified Information

Hugh George HAMBLETON - HAMBLETON was convicted of espionage in 1982 and sentenced to 10 years in prison. At the time of his arrest he was a professor of economics at Laval University, Quebec City, Canada. He was alleged to have passed thousands of NATO classified and unclassified documents to the Soviet KGB while working in NATO from 1956 to 1961. Eighty of the documents involved in HAMBLETON's espionage activity were classified NATO TOP SECRET. HAMBLETON grew up in affluent surroundings and had social status both in Canada and Western Europe. His mother had become enamoured with Russian culture and history and socialized with Soviets on the continent and in Canada. At 29 years of age HAMBLETON was introduced to a Soviet diplomat at one of his mother's social functions. The diplomat, a Soviet intelligence officer, cultivated HAMBLETON and eventually recruited him with the instruction to obtain NATO employment. HAMBLETON was successful in obtaining employment in the Economics Section of NATO Headquarters. During World War II HAMBLETON had worked for French, U.S. and Canadian intelligence and had enjoyed these experiences. His work for the Soviets was an extension of the influence of his mother's fascination with the Russian culture and his own sense of adventure which was satisfied by playing the role of a spy.

Geoffrey Arthur PRIME - This British citizen was sentenced in November 1982 to 35 years imprisonment for espionage conducted on behalf of the Soviet KGB. He volunteered his services to the Soviets in 1962 while an enlisted man stationed in Berlin. His last assignment prior to his arrest was as a civilian translator of coded Russian radio traffic at Britain's electronics communications center, the Government Communication Headquarters. Although this was not a NATO assignment, the communications center handled highly classified NATO information and PRIME is thought to have revealed information dealing with NATO military strength figures, status of equipment, and clandestine NATO agents. PRIME had become sympathetic to Marxist teachings as a result of his under-privileged status as a youth and by having listened to Russian and German language broadcasts emanating from the East Bloc. Although paid for his services, ideology was the basic motivational factor in his willingness to be recruited by Soviet intelligence.

Vladimir ZOLOTARENKO - This French citizen was of Russian heritage and as a young man frequented Russian restaurants and bookstores in Paris. At a chance encounter in such a bookstore, ZOLOTARENKO was befriended by a Soviet diplomat and eventually introduced to a second Soviet who recruited ZOLOTARENKO for the KGB. ZOLOTARENKO was employed as a reproduction specialist at the Advisory Group for Aerospace Research and Development (AGARD), where he had access to, and provided to KGB, a variety of NATO classified and unclassified documents. He also passed to the KGB information concerning his co-workers at AGARD, information on the lay-out of the building and various activities of the agency. ZOLOTARENKO's cooperation with Soviet intelligence was principally ideological although money also played a factor.

Gunther GUILLAUME - While serving as a personal assistant to Willy Brandt, then Chancellor of the Federal Republic of Germany, GUILLAUME was discovered to be an officer in the East German intelligence service. Strictly speaking this is not a NATO case or a recruitment effort since GUILLAUME was an East German penetration agent. He undoubtedly had access to and compromised, NATO-related information.

Francis ROUSSILHE - While head of the Registry of the International Secretariat, NATO, ROUSSILHE, a French citizen, provided almost 5,000 NATO documents to the Rumanian Intelligence Service.

Nahat IMRE - A Turkish official, IMRE was financial comptroller for the International staff at NATO Headquarters. He had direct access to the most highly classified NATO activities and when arrested in 1968, he was in possession of numerous NATO documents. He had been working for several East European intelligence services from the late 1950's until his arrest.

George PAQUES - Recruited by the KGB at the end of World War II, PAQUES held several senior positions in the French Government and in 1958 became a member of the French Ministry of National Defense. Subsequently, in 1962, PAQUES became deputy director of NATO's press and information service where he remained until his arrest in August 1963.

Leonore Heinz SUETTERLIN - This unmarried secretary in the West German Foreign Office was wooed and wed by SUETTERLIN who, unknown to her, was an agent of the KGB. She provided to her husband more that 3,000 documents from her office including Foreign Office cable traffic and NATO and German defense and intelligence information. She also provided personalia on other foreign service employees and on security investigations of Soviet and East German agent suspects.

Alfred FRENZEL - A sitting member of the Social Democrat Party MP, FRENZEL was recruited by Czech intelligence in 1956. Until his arrest in 1961 FRENZEL provided the Czechs information on the German defense budget and defense plans, the organization of the Army and Air Force, reorganization plans for the German Navy, German rocket and aircraft projects, and data on items of NATO equipment. His confession indicated that he engaged in espionage primarily for reasons of ego although he was paid for his efforts.

Giorgio Rinaldi GHISLIERI - GHISLIERI, an Italian citizen, worked for Soviet intelligence from 1956 to 1967. He and his wife established a network of agents to report on NATO bases in Italy and U.S. Air Force bases in Spain.

Rear Admiral Hermann LUEDKE - Until January 1968 LUEDKE was Deputy Chief, Logistics Division, NATO. While in this position he photographed NATO classified documents for his Soviet controllers. Several days following his confrontation on charges of espionage he was found dead, apparently a suicide.

Renate and Lothar LUTZE - This West German couple both worked for Defense and passed over 1,000 secret documents to East German intelligence of which one fifth dealt with NATO information, including information on its nuclear weapons and plans for dealing with a Communist offensive in Western Europe . The LUTZE's were arrested in 1976 and subsequently Lothar was sentenced to 15 years in prison while Renate was given an 11 year sentence.

Marie-Luise and Horst SCHADOCK - Arrested in 1977, the SCHADOCK's were found to have been an East German penetration team who had worked for several years in German and NATO defense installations.

Ursel LORENZEN - This German secretary, who had been working in NATO Headquarters since 1966, defected to East Germany in 1979. It is believed that she provided to the East Germans all NATO information to which she had access. It was reported that LORENZEN took details of a NATO Command Post exercise "WINTEX" with her when she defected. It was subsequently reported that LORENZEN had spied "for love" and that she married her former East German spymaster following her defection.

Gerda SCHROETER - A secretary in the West German State Department, Gerda SCHROETER, confessed in 1973 that she had been an espionage agent for East Germany for eight years. During that time SCHROETER had worked in the coding and communications department of the State Department at Bonn and had spent a short time in the FRG Embassies in Washington and Warsaw. Material which she furnished to the East Germans included NATO information. SCHROETER was recruited for espionage work at a young and impressionable age based on ideological persuasion.

Imelda VERREPT - A Belgian secretary at the International Secretariat, NATO Headquarters, Imelda VERREPT defected to East Germany in April 1980. VERREPT had been employed as a typist in the secretarial pool. It was reported at the time that VERREPT sought asylum in East Germany on grounds of conscience because of "the dangers of NATO policies." She had access to "many hundreds of secret plans" including "measures of the Nuclear Planning Group to 'Modernize' NATO medium-range nuclear weapons on the battle scene." East German newspapers published photographs of documents which VERREPT allegedly took with her including a COSMIC (TOP SECRET) targeting document.

Azeglio NEGRINO - NEGRINO was a ranking official of Microlito, an Italian microfilm company, with access to classified military documents, weapons designs and models, and military installations. At the time of his arrest in February 1983, NEGRINO was in possession of hundreds of such documents and microfilm, including plans for a new NATO air weapon and pictures of several NATO installations in Italy. The Italian and NATO classified information was intercepted by Italian security authorities while being passed to a Soviet contact. He allegedly handed over microfilm containing 50,000 pages of SECRET documents. NEGRINO stated that he had been contacted by the KGB the previous year and pressured into cooperating in exchange for money.

Frederic SAUSSEZ/Marcel BARBIER/Michel LIBERT - These three individuals were not engaged in espionage but rather stole classified documents for extreme right-wing causes. Material taken by SAUSSEZ, a member of the new-Nazi organization Westland New Post, included NATO SECRET documentation.

Ingrid GARBE - GARBE worked as a secretary in the West German Mission to NATO from 1976 until her arrest in 1979. She was recruited by an East German intelligence officer with whom she had fallen in love. GARBE had worked for EGIS for eight years. She originally applied for work with the West German Foreign Ministry at the direction of EGIS.

Horst JONAS - On 14 May 1982, West German national Horst JONAS was sentenced to four years imprisonment for intelligence collection activities on behalf of the Soviet Intelligence Services. Among information/items sought by JONAS were those pertaining to the classified fire-control and anti-missile system of the Phantom aircraft utilized by the various NATO countries.

Irmgard ROEMER - Recruited by the East German Intelligence Service in approximately 1958, ROEMER was a victim of East German utilization of romantic motivations. While working in a communications center handling incoming and outgoing communications for West German embassies, ROEMER provided carbon copies of the communications to her handlers.

Horst MAEMECKE - A West German code expert, MAEMECKE was arrested in April 1983 on charges of espionage performed on behalf of the Soviet GRU. MAEMECKE admitted to having been recruited by the GRU during an unauthorized visit to East Germany in 1976. He stated that in 1981 he passed to the GRU a list of communications codes for the West German Army's Southern Sector.

Erhard MUELLER - A former West German naval officer, MUELLER defected to East Germany in 1978. He stated in an East German television interview that he had worked in a secret U.S.-West German intelligence group whose function was disinformation/propaganda regarding the Soviet military threat. He stated that other NATO member nations did not know of this group's existence. MUELLER had access to aerial photographs taken by a naval reconnaissance squadron stationed at Eggebeck near the Baltic Sea.

Serge FABIEW - A naturalized French citizen, FABIEW was born in Yugoslavia and headed a spy ring in Paris. In 1978 FABIEW was sentenced to 20 years in prison for having passed information on French aviation matters and on NATO committees on arms supplies and advanced technical research. One of the ring, an Italian named FERRERO, also passed NATO related material and stated he was motivated solely by money.

Heinz Bernhart ZORN - ZORN was a retired Major General, East German Air Force, who traveled to France on a tourist visa to perform espionage tasks. At the time of his arrest in August 1980 ZORN was in possession of information on French tanks and anti-tank weapons.

Sahag K. DEDEYAN - DEDEYAN, a naturalized U.S. citizen, provided a distant relative with national defense documents for delivery to the Soviet Union. DEDEYAN was a DoD contract employee with a TOP SECRET clearance. Among the documents he and his relative passed was a SECRET study entitled "Vulnerability Analysis; U.S. Reinforcement of NATO." The pair was arrested in 1975 on charges of having performed espionage since 1971 on behalf of the Soviets.

Norbert MOSER - A West German Air Force Colonel, MOSER was arrested in 1975 after having worked for East German intelligence for 17 years. MOSER was sentenced by a West German court to 11 years in prison.

Name/Nationality	Dates of Intel Activity	Position/Compromises	Hostile Service	Motivation
George Paques French	1945-1963	Dep Dir, Press & Info Service, NATO	KGB	Ideology
Gunther Guillaume East German penetrant	1955-1974	Personal Assistant to FRG Chancellor	EGIS	Ideology
Hugh George Hambleton Canadian	1956-1982	Economics Section, NATO Hqs (56-61)	KGB	Adventure/ideology
Alfred Frenzel West German	1956-1961	Sitting member of SDP	CIS	Ego/monetary
Giorgio Rinaldi Ghislieri Italian	1956-1967	Reported on NATO bases in Italy	SIS	Monetary
Nahat Imre Turkish	1958-1968	Comptroller, Int'l Staff, NATO	Several WP Intel Services	Monetary
Irmgard Roemer West German	1958-?	Embassy Comm Center	EGIS	Romance
Norbert Moser West German	1958-1975	LTC, West German AF	EGIS	?
Leonore Heinz Suetterlin West German	1960-?	Secretary, FRG	KGB	Romance
Vladimir Zolotarenko French	1962-1980	Reproduction spec, AGARD	KGB	Ideology/monetary
Geoffrey Arthur Prime British	1962-1981	Government Communications Headquarters	KGB	Ideology/monetary

Name/Nationality	Dates of Intel Activity	Position/Compromises	Hostile Service	Motivation
Serge Fabiew French (naturalized Yugoslavian)	1963-1974	Headed spy ring	KGB	Monetary (one member of spy ring stated he was motivated solely by mone
Gerda Schroeter West German	1965-1973	Secretary, FRG State Dept	EGIS	Ideology
Renate and Lothar Lutze West German	1967-1976	FRG Defense	EGIS	?
Francis Roussilhe French	1960's	CH, Registry of Int'l Secretariat NATO	RIS	?
Hermann Luedke West German	?-1968	Rear Admiral, Dep Ch, Log Div, NATO	SIS	?
Sahag K. Dedeyan (naturalized US)	1971-1979	DoD contract employee	SIS	Monetary (relationship passed documents to distant relative)
Ingrid Garbe West German	1971-1979	Secretary, FRG Mission to NATO	EGIS	Romance
Marie-Luise and Horst Schadock East German penetrants	1974-1977	Penetrated German and NATO defense installations	EGIS	Ideology
Horst Maemecke West German	1976-1983	Code expert	GRU	?
Erhard Mueller West German	?-1978	FRG Naval Officer	Defected to East Germany	Ideology

Name/Nationality	Dates of Intel Activity	Position/Compromises	Hostile Service	Motivation
Heinz Bernhart Zorn East German	1978-1980	Retired MG, GDR AF	Performed espionage for GDR against France and Belgium	Ideology
Azeglio Negrino Italian	1982-1983	Microfilm progressor w/defense contract	KGB	Pressure/monetary
Saussez/Barbier/Libert Belgian	1983	Civilian and military	Stole documents for extreme right-wing causes	Ideology
Horst Jonas West German	?-1982	Sought info on weapons systems	SIS	?
Ursel Lorenzen West German	?-1979	Secretary, NATO Hq	EGIS (defected to East Germany)	Romance
Imelda Verrept Belgian	?-1980	Secretary, NATO Hq	EGIS (defected to East Germany)	Romance/ideology

RECORD VERSION

STATEMENT FOR THE RECORD BY

OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
HEADQUARTERS, DEPARTMENT OF THE ARMY

FOR THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
U.S. SENATE

FIRST SESSION, 99TH CONGRESS

DEPARTMENT OF THE ARMY PERSONNEL SECURITY PROGRAM

26 FEBRUARY 1985

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

STATEMENT FOR THE RECORD

DEPARTMENT OF THE ARMY PERSONNEL SECURITY PROGRAM

I. Program Overview.

a. The Department of the Army's Personnel Security Program (PSP) is conducted in accordance with the authority contained in Department of Defense Directive and Regulation 5200.2, entitled, "Department of Defense Personnel Security Program." The terms of that Directive and Regulation are promulgated, with limited supplementation, as Army Regulation 604-5.

b. The purpose of the program, as stated in AR 604-5, is:

"To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense (DOD), and granting members of the Armed Forces, DOD civilian employees, and other affiliated persons access to classified information are clearly consistent with interests of national security."

c. The proponent agency for conducting the PSP within the Army is the Office of the Assistant Chief of Staff for Intelligence (OACSI), Headquarters, Department of the Army.

d. There are three basic areas which constitute the PSP. The first is identification of positions, the incumbent of which will require access to classified information or other sensitive material. The second is the conduct of a personnel security investigation which varies in scope depending on the nature and sensitivity of information to which the incumbent will have access. The third is adjudication of information developed by the investigation to determine if specified standards of responsibility, reliability, trustworthiness, and loyalty are met.

e. All persons entering the Army and all civilian employees undergo a nominal investigation to establish their eligibility for entry or employment. A National Agency Check (NAC) is conducted prior to appointing commissioned or warrant officers. An Entrance NAC (ENTNAC) is conducted on all enlistees at the time of their entry. A NAC with written inquiries (NACI) is conducted on all civilian applicants, with some limited exceptions.

f. If a person will require access to information classified TOP SECRET, or other highly sensitive information, a Background or Special Background Investigation (BI/SBI) may be required. NACs and ENTNACs on military personnel are conducted for the Army by the Defense Investigative Service (DIS). NACIs for civilian employees are conducted by the Office of Personnel Management (OPM). BIs and SBIs are also conducted by the DIS.

g. Civilian employee positions consist of three categories - nonsensitive, noncritical-sensitive, and critical-sensitive. A NACI is conducted on applicants for nonsensitive and noncritical-sensitive positions. A BI is conducted on applicants for critical-sensitive positions. Determination of eligibility for employment is made by the servicing civilian personnel management office.

h. Military positions are not categorized like civilian positions. A BI or SBI is conducted only when assigned duties require access to material classified TOP SECRET or designated as Sensitive Compartmented Information (SCI), or duties include such activities as conducting investigations or performing White House support functions. The determination of eligibility for entry into the military service is made by military personnel management officials.

i. The prerequisite investigation for establishing eligibility for access to material classified SECRET is a NAC, ENTNAC, or NACI. Eligibility for access to TOP SECRET material is based on a BI; an SBI is conductd on persons requiring access to SCI. All determinations of eligibility/ineligibility (adjudications) for access to classified material (all levels) are made by the U.S. Army Central Personnel Security Clearance Facility (CCF), Fort Meade, MD. These determinations are made on personnel in the Active Army, U.S. Army Reserve, Army National Guard, and civilian employees. The only determinations made on contractor employees are for access to SCI.

j. Personnel security clearance determinations on contractor personnel for access to SECRET and TOP SECRET material are made by the Defense Industrial Security Clearance Office (DISCO), Columbus, OH. All personnel security investigations on contractor personnel are conducted by the DIS.

II. Importance of personnel security.

a. National security requires that persons in positions of special trust be of established integrity, trustworthiness and discretion. Similarly, persons afforded the opportunity to serve in the Armed Forces must demonstrate good conduct and character, be reliable and of unswerving loyalty to the United States. A time-proven way of determining these personal characteristics is to conduct a comprehensive review (personnel security investigation) of their suitability and qualifications to hold such sensitive positions.

b. The personnel security program is the only viable means of achieving this goal. Without it, chaos would exist. Protection of our nation's most sensitive information would be virtually non-existent. National security would become national vulnerability. Pursuit of a vigorous personnel security program is absolutely necessary to the conduct of good government and effective Armed Forces.

III. Issues.

1. Effectiveness of Executive Order 10450.

a. EO 10450 uses the terms "sensitive position" and "National Security" which, at the time of issuance and for many years afterwards, did not appear to require further definition. At this time, because of various policy and judicial developments, there is a perception of doubt as to whether national security means only positions which require access to classified information or also means positions that involve sensitive duties which do not require access to classified material, e.g., law enforcement and fiduciary. This issue is being examined by a study group convened as a result of National Security Decision Directive on Safeguarding National Security Information (NSDD-84).

b. EO 10450 is directed at Federal officers and employees, leaving the applicability of it to the military sector in doubt. Whereas the provisions of the EO are sound, we feel that one of two courses of action should occur: (1) expand the applicability to include the members of the Armed Forces, or (2) strive for a new EO which specifically applies to the Armed Forces.

2. Ability to detect from a Background Investigation potential security risks.

a. There are several different scopes of BIs for various levels of clearance. All of them entail a check of the Federal Bureau of Investigation (FBI) and the Defense Central Index of Investigations (DCII). This is to ascertain if a criminal record exists at the national level or if other agencies have conducted an investigation of any type. Other agency checks follow if so identified in the DCII.

b. More detailed investigations include interviews of former employers/supervisors, educational references, and developed references. Checks are also made of employment, credit and educational records and local law enforcement agencies. BIs for military personnel and contractor employees include a personal interview of the subject of investigation.

c. All of these investigations are conducted to ascertain the nature of the individual's loyalty, character, reliability, discretion and trustworthiness. Security clearance determinations are made on the basis of demonstrated conduct, but no amount of investigation could ensure reduction of the security risk to zero or establish that a person who has been granted a security clearance will remain trustworthy.

d. During FY 1984, the Army granted 259,000* security clearances; that same period, the Army denied or revoked 5,400* clearances. Of the 5,400* denials and revocations, we estimate that approximately 50% were based on personnel security investigations. This translates as some 2,700 persons having been nominated for access to classified information, or having had a security clearance granted earlier, who for one reason or another failed to measure up to required standards and thus were denied a security clearance or had their security clearance revoked because they constituted an unacceptable security risk.

e. The scope of BIs conducted on military and contractor personnel includes a personal interview of the subject of investigation. The scope of the investigation conducted on Federal employees, however, does not routinely include an interview of the subject of investigation. The so-called Interview-oriented investigation has proven to be valuable in acquiring personal information that otherwise would possibly not have been developed in the standard non-interview investigation. Addition of the interview to the investigation conducted on Federal employees could serve as a meaningful move.

* Figures are rounded

3. Programs addressing the continuing assessment of personnel with clearances and access.

a. An inherent aspect of a strong personel security program is command and supervisory oversight of subordinates with security clearances. A complementary aspect is the conduct of periodic reinvestigations. The oversight issue is addressed in AR 604-5 under the section entitled, "Continuing Security Responsibilities" (Chapter IX). Periodic Reinvestigations are not conducted on all persons having a security clearance, but they are conducted on those persons having access to the most sensitive material. These groups include persons having access to SCI, persons engaged in White House Support activities, persons having access to Single Integrated Operation Plans - Extremely Sensitive Information (SIOP-ESI), and persons assigned to North Atlantic Treaty Organization (NATO) elements. The requirement for the conduct of Periodic Reinvestigations is also addressed in AR 604-5.

b. In paragraph 2d, above, we estimated that approximately 50% of denial and revocation actions were based on personnel security investigations. The remainder of the denial and revocation actions is based on information resulting from command and supervisor oversight. Our security procedures require that, when adverse or derogatory information surfaces, on civilian or military personnel, it will be reported to the CCF for review and possible reconsideration as to continuing eligibility to hold a security clearance.

4. Investigative procedures and techniques.

a. NACIs for civilian employees are conducted by the OPM. BIs and SBIs on all categories of Army affiliated personnel are conducted by the DIS, as are entry level NACs and ENTNACs for military personnel. NACs, ENTNACS, and NACIs are initiated by personnel security officials. A chronic problem associated with the conduct of personnel security investigations is timeliness of completion.

b. OPM reports that it completes NACIs in approximately 45 days. On the surface this does not appear to be major problem but when processing and transmission time are added, it is usually more than 75 days from date of initial dispatch to receipt of the final results. When considering that the NACI is required to be completed before actually employing an applicant for a critical-sensitive position, it can be seen that many talented applicants are lost because of the extensive lapse of time during which the applicant tires of waiting and seeks employment elsewhere. A second problem with NACIs is that many sources from which OPM attempts to acquire information neglect to return the OPM inquiries. This, of course, is a situation over which OPM has no control, but it results in the closing of a NACI in many cases with very incomplete information. Those sources whom the OPM queries are former employers, former places of education, and local law enforcement agencies where the subject of investigation has resided.

c. DIS-conducted NACs and ENTNACS require approximately 35-40 days to complete. In the case of applicants for appointment as officers and warrant officers, this does not constitute a problem. In the case of new enlistees, however, we find that many soldiers enlist under fraudulent conditions and this is discovered only after substantial sums have been spent on processing the soldier and possibly even training him/her. The Office of the Secretary of Defense (OSD) is currently engaged in an action to automate the conduct of ENTNACs, activation of which should reduce ENTNAC completion time substantially - to approximately 5-10 days.

d. DIS-conducted BIs and SBIs are currently being completed in approximately 90-95 days against an OSD goal of 65 days. When transmission and adjudication time are added, a total lapse time of 120+ days occurs. This often results in soldiers arriving at new duty stations and not being eligible to perform their duties because of the system's inability to grant a security clearance in a timely manner.

The obvious result is an adverse impact on the unit's ability to properly accomplish its mission, degradation in morale of the soldiers involved, and an unacceptable amount of non-productive time for the soldiers. Lengthy case completion times have come about because of an increasing case load at DIS.

e. As regards investigative techniques, the Army is confident that DIS investigators are adequately trained and the DIS exercises good quality control in the conduct of its investigations.

5. Adjudicative procedures and techniques.

a. When the DIS completes a personnel security investigation for an Army civilian employee or member of the Active Army, U.S. Army Reserve, or Army National Guard, it is forwarded to the U.S. Army Central Personnel Security Clearance Facility (CCF) for adjudication. The CCF makes all security clearance and SCI eligibility determinations for Army-affiliated personnel except for contractor employees. Security clearances for contractor employees are granted by the Defense Industrial Security Clearance Office, Columbus, OH but SCI eligibility determinations on this category are made by CCF.

b. Information developed by the DIS investigation is considered by the CCF adjudicator against detailed adjudication guidance which is contained in AR 604-5 (Chapter VI and Appendix I). The guidelines were developed by OSD and are used by all DOD components in personnel security clearance actions. They may be considered somewhat judgmental and subject to different interpretation by different agencies, but this is acceptable in that they provide sufficient latitude to accommodate mitigating factors in a given case.

c. When a favorable clearance determination is made, CCF notifies the parent unit of the subject involved that a security clearance is granted. If an unfavorable determination is made, due process procedures are triggered. Due process is discussed below.

6. Due process procedures - problem areas.

a. When a personnel security investigation discloses information which casts credible doubt as to the trustworthiness, reliability, integrity and/or loyalty of the subject of investigation to the extent that a risk to national security is perceived, the CCF prepares a Letter of Intent to Deny or Revoke Security Clearance. The letter presents a summary of the adverse information which constitutes the basis for the initial determination and is forwarded to the individual concerned through command channels. The letter offers the individual the opportunity to advise of mitigating, explanatory, or refuting information. If the individual declines to respond to the Letter of Intent, the revocation or denial becomes final. If he/she chooses to challenge the charges presented in the Letter of Intent, his/her response is returned to CCF through command channels.

b. Upon receipt of the individual's response, CCF reconsiders the merits of the case and makes a final determination. If it is favorable, CCF notifies the person's organization that a clearance has been granted. If it is unfavorable, CCF forwards a letter of final determination, through command channels, to the individual. This letter informs the individual that he/she may appeal the CCF determination to Headquarters, Department of the Army, and provides the proper mailing address for this purpose.

c. Of the 5,400 clearance denial/revocation actions taken by CCF in FY 1984, 83 persons chose to appeal their cases to HQDA. Of those, 38 were decided in favor of the individuals and the remaining 45 denials/revocations were upheld.

d. We perceive no major problems with the due process system now in effect within the Army. For the most part, appeals to HQDA are well documented and provide sufficient information for detailed re-evaluation. Very few are frivolous in nature or imply a "what do I have to lose" attitude. In all cases where a security clearance is revoked, the person's access to classified material is suspended during the appeal process. In such cases, the individual is obviously not performing in his/her primary skill, thus productive time is lost to the Army. Fortunately, the number of such cases is so small that the loss in terms of man-days is nominal.

7. Position as to the use of a polygraph.

a. The Army supports the use of the polygraph for personnel security screening as an augmentation to the normal personnel security investigation. We do not feel that it should be used as a sole basis for granting or denying access to classified material.

b. We also feel that the scope of the examination should be limited to counterintelligence/loyalty type questions. Whereas so-called "life style" questions may result in acquisition of adverse suitability information, this type information may also be derived from traditional investigation techniques. Limitation of the examination to counterintelligence and loyalty thus circumvents the possible perception of invasion of privacy.

8. Position as to psychological evaluation.

a. Psychological screening of candidates for assignment to high risk or high stress jobs serves many useful functions. The ability to identify individuals at the entry level who may not be suited for the peculiar stresses of such positions saves valuable time and resources.

b. The usefulness of psychological screening as a tool for predicting future job performance has been demonstrated by its ability to provide valuable information about individuals' vulnerabilities, controllability, and decision making styles that are not assessible during routine investigation and clearance procedures. Use of a screening battery during the selection process will not provide for perfect decisions nor completely eliminate errors, but the process will minimize the degree to which we are taken by surprise and create a selection program that is self-corrective in nature.

9. Impact of the Merit System Protection Board in personnel security matters.

a. In late 1983, the MSPB advised that, henceforth, it will apply the standard enunciated by the D.C. Circuit Court in HOSKA V. DEPARTMENT OF THE ARMY (677 F.2d 131)(D.C. Cir. 1982). That standard held that the removal of an employee whose security clearance is revoked is lawful only if the revocation was lawful. To be lawful, there must be a rational nexus between the denial or revocation of a security clearance and the conduct or other evidence relied on by the government in denying or revoking the clearance.

b. At this time, questions have arisen concerning whether the MSPB has the authority to review the agency's stated reasons for revoking or denying a security clearance, and whether the MSPB has the authority to order the agency to reinstate a security clearance.

c. Close examination of these issues has been launched by the MSPB by inviting interested agencies to submit briefs no later than 14 February 1985. The Army sides with those who feel the board does not have the authority to review the merits of a clearance denial or revocation determination or to substitute its judgment for the expert conclusions of the agency.

10. Secret Clearances.

a. The investigative basis for a SECRET clearance is a NAC, ENTNAC, or NACI. The scope of the NAC and ENTNAC is limited to a check of the DCII, FBI, and such other agencies that may have records on the subject of investigation, as identified through the DCII and FBI checks. The NACI consists of the same checks as NAC/ENTNAC and also includes written inquiries to former employers, former places of education, and law enforcement agencies in areas where the subject of investigation resides or has resided in the past.

b. These three types of investigations are conducted at the time a soldier (enlisted or commissioned) or a civilian employee first affiliates with the Army. For the purpose of granting a SECRET security clearance, the entry investigation satisfies the investigative requirement. Only if there is a break in service (military or civilian) of one year or more, must a new investigation be conducted. Once the investigation is conducted and the person continues unbroken affiliation with the Army, the entry investigation satisfies the investigative requirement for a SECRET clearance - even if it is five or ten years old. This is seen as a weakness in the system because a person's lifestyle and philosophies can change drastically with the passage of only a few years. The Army would support the conduct of a new investigation to serve as the basis for granting a SECRET clearance if the old investigation was more than two years old and the subject had not previously held a security clearance.

c. Whereas the scope of a NACI, if all vouchers are responded to, is considered adequate investigation for the granting of a SECRET clearance, the weakness here is when persons queried fail to respond and the NACI is closed without the benefit of the desired background information. In this situation, the NACI becomes no more than a NAC or ENTNAC.

d. The scope of the NAC/ENTNAC is considered deficient by checking only the agencies noted in paragraph 10a, above. As a minimum, we would subscribe to the addition of a personal interview of the subject of investigation to ensure current information from the individual him/herself.

e. As noted in paragraph 10b, above, once an investigation has been conducted it remains valid for as long as the person sustains unbroken affiliation with the Army. A reinvestigation is neither required or conducted on persons having SECRET clearances and, once granted, the clearance can remain in effect for 20 to 30 years. We feel that this is also a weakness in the system and recommend a new investigation be conducted every five years.

f. Some persons in the security community have noted that a number of people with SECRET clearances have very little actual access to classified material, whereas others have extensive, daily access to such material. The question arises, should those with the more extensive access have a broader scope investigation than those with limited access? In our view, the damage that can be done to national security by the unauthorized release of one SECRET document may often be just as serious as the unauthorized release of multiple documents. Accordingly, we feel that a uniform investigation for the granting of a SECRET clearance, regardless of magnitude of access, is the preferable option.

11. Effectiveness of the National Agency Check.

a. The NAC continues to be a relatively valuable investigation. There is one major deficiency with it in that the forwarding of criminal information to the FBI by local law enforcement agencies appears to be an optional action. Because of this, a person could have a record of serious dimensions at the local level, but it would not necessarily be recorded at the FBI. The NAC, of course, does not encompass checks of local law enforcement agencies.

b. It would be extremely beneficial not only to the intelligence community, but also the criminal justice community if legislation could be developed which causes serious crime reporting to the FBI to be mandatory.

12. Government oversight of personnel security of contractors.

a. It is absolutely essential that government oversight of personnel security matters concerning Defense contractors be exercised continuously and vigorously. Only such oversight can ensure adherence to established policy and procedures and avert abuse of the system by clearing more persons than are actually needed to perform the contract. Every additional, unnecessary investigation results in unnecessary costs and expenditure of investigative resources.

b. The Defense Investigation Service (DIS) currently exercises oversight of contractors in behalf of the various Defense components. Each contractor is assigned an Industrial Security Representative (ISR) who is charged with conducting the oversight.

13. Ambiguity in dealing with security and suitability matters.

a. The emphasis on suitability for employment rests on an individual's ability to perform the functions of the position, as determined by education, training and experience. Suitability as regards security, on the other hand, is dependent on exhibited character traits that reflect loyalty, trustworthiness, reliability, discretion and integrity.

b. Ambiguity arises when an employee's (usually) off-duty conduct conflicts with the security standards. If the individual's position requires a security clearance and the person can ably perform the duties of the position, personnel management considers him qualified for the position as long as his/her off-duty conduct does not affect job performance.

c. Conflict often arises when a person in a position which requires a security clearance performs an act or acts of such gravity that revocation of the security clearance is recommended or accomplished. In many cases, when a security clearance is revoked, it becomes necessary to separate the employee because positions of similar grade and skills cannot be found by the employing agency.

IV. Deficiencies and problems. These areas have been covered in paragraph III, above.

STATEMENT OF
REAR ADMIRAL JOHN L. BUTTS
DIRECTOR OF NAVAL INTELLIGENCE
BEFORE THE
SENATE GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON INVESTIGATIONS
ON
DEPARTMENT OF THE NAVY PERSONNEL SECURITY PROGRAM

I am Rear Admiral John Butts, Director of Naval Intelligence. I am the official designated by the Secretary of the Navy to be responsible for ensuring an effective personnel security program in the Department of the Navy (DON).

The foundation of all of our security efforts is the personnel security program. Administrative and physical security measures designed to protect the classified information of the Navy and the government are not effective if the people given access to the information are not reliable, trustworthy and loyal. Thus, the objective of our personnel security program is to ensure, to the maximum extent possible, that individuals given access to sensitive information are indeed trustworthy and reliable. To this end, Navy has issued an instruction, "Department of the Navy Information and Personnel Security Program Regulation" (OPNAVINST 5510.1G), which implements Secretary of Defense policies aimed at identifying those individuals who may be properly given access to classified information.

Personnel security determinations begin with an evaluation of the duties assigned to an individual and whether those duties will require the individual to be cleared for access to classified information. If so, an investigation of the individual is initiated. The scope of the investigation will depend on the level of clearance required. If the individual requires access to information up to the Secret level, a National

Agency Check by the Defense Investigative Service or a National Agency Check with Written Inquiry by the Office of Personnel Management is conducted. If access up to the Top Secret level is required, a more in-depth Background Investigation by the Defense Investigative Service is conducted. The results of these investigations, as well as any other available information in respect to the individual's behavior, character and personal circumstances, are reviewed in light of the security criteria and adjudication guidelines established by the Secretary of Defense and implemented in the Navy by the Navy instruction cited above. If it is proposed to deny an individual security clearance, he or she is given an opportunity to appeal a decision to deny clearance.

The requirement to ensure the propriety of each individual's clearance and access is continuing and is as important as the original determination to grant access. Accordingly, our regulations require: (1) each Commanding Officer maintain a program for continuous evaluation of the propriety of an individual's clearance and access to classified information; (2) determination authorities be advised of any information which bears on a cleared individuals's trustworthiness and reliability so the individual's continued eligibility may be assessed in light of the additional information; and (3) individuals with access to Top Secret information be re-investigated at regular intervals.

Inasmuch as most of our adverse personnel security determinations are revocations of clearance or access vice initial denials, our continuous assessment and review programs appear to be practiced and effective. Again, if it is proposed to revoke an individual's clearance or take any other adverse personnel security action against an individual, the individual is provided an opportunity to respond to the proposal and to appeal any negative determination.

The quantity and quality of information available for evaluation obviously are key to an effective personnel security investigative program. The National Agency Check is limited in scope. It gleans information of record in the national agencies checked but, in the absence of previous files, it provides no information bearing on trustworthiness. No field investigation is done unless unresolved derogatory information is disclosed. The majority of NAC's report that there is no national record information on the individual. Espionage cases prove how damaging the loss of Secret information can be and have brought into question the sufficiency of the NAC as the investigative basis for allowing access to Secret. More information bearing on trustworthiness would be desirable but additional requirements for investigation or reinvestigation cannot be met by the Defense Investigative Service within present administrative and investigative resources. The more extensive Background Investigation provides clearance adjudicators with significantly more information upon which to base the clearance adjudication determination.

Personnel security specialists and behavioral scientists agree there is a real need for personnel security research to identify indicators of security significance and to develop investigative procedures and techniques to acquire the information which will reveal these security indicators. One type of personnel security research being pursued with Intelligence Community funding is after-the-fact examinations of those who were involved in espionage. This research is attempting to identify patterns of behavior and character that could be used to identify security risks which would not have been discerned under our present screening and investigative process.

Security criteria and adjudicatory guidelines established by the Office of the Secretary of Defense are applied by all DOD activities. The security criteria and adjudicative guidelines are used to identify those characteristics of individuals under investigation for access to classified information which may indicate the individual is untrustworthy. While the criteria and guidelines are of value to the security clearance adjudicative determination process, we need to better understand and identify the characteristics of security significance and to provide better training of adjudicators. The Intelligence Community has addressed the training aspect by holding SCI adjudicator conferences three times a year, but many adjudicators must rely on experience as their only teacher. A training program for DOD adjudicators is needed.

Psychological evaluations more clearly establishing an individual's motivations and emotional stability, as well as providing a better understanding of the significance of particular behavior, when combined with the results of the basic investigation, would greatly enhance our security clearance adjudication processes. Unfortunately, we do not presently have the resources to routinely incorporate psychological evaluations into the security clearance determination processes, but may only use such evaluations in those cases when necessary to resolve issues of mental or emotional instability. Efforts are underway within the Department of Defense to identify psychological testing methodologies which could be of use in lieu of time-consuming, expensive psychological interviews and yet still provide some basis for evaluating the psychological and emotional state of the individual to be cleared.

We consider the polygraph to be a valuable and effective tool for specific personnel security purposes. The polygraph is particularly useful in assessing candidates for access to our most sensitive information and for periodic reassessment of such individuals. Polygraph questioning is limited, pursuant to DoD policy, to counterintelligence questions. Further, in the Navy, individuals who refuse to submit to a polygraph examination will not be subjected to adverse actions or adverse personnel security determinations solely on the basis of their stated refusal. We believe the use of the polygraph in this manner permits an appropriate balance between the needs of national security and individual rights.

Whenever an adverse personnel security determination is made, administrative due process is provided to the affected individual. This due process consists of the following:

1) The individual concerned is given a written statement of intent to deny/revoke clearance.

2) The individual is given an opportunity to submit a written statement in his own behalf. The statement is submitted via the commanding officer who is encouraged to state the command's recommendations.

3) The individual is provided a written statement of the decision.

4) The individual may appeal the denial/revocation to higher authority. The appeal is also submitted via the commanding officer for comment or recommendation.

We feel the procedures are sufficient and fair. They allow the individual to provide comments and have them considered with respect to the actual decision, the rationale behind the decision, and the information upon which the decision is based. Furthermore, to ensure that the views of the individual's superiors are considered, i.e., the views of those most familiar with the individual, the individual's commanding officer is also given the opportunity to comment during the review process.

Personnel security determinations are and must remain the responsibility of the Navy. However, recent decisions of the Merit Systems Protection Board (MSPB) have demonstrated that they have assumed jurisdication to review security clearance denial/revocation decisions when a civilian employee appeals his or her removal from employment subsequent to the security clearance denial/revocation. In several cases the MSPB has ordered the Navy to reinstate the employee and to restore the security clearance. In one case, the MSPB went so far as to order the Navy to restore clearance and to give the particular individual concerned access to classified information.

The Navy has objected to these decisions. These objections are grounded in both principles of law and principles of sound security management. Security professionals are best suited to evaluate the propriety of a particular individual's access to classified information. If Navy is required to comply with MSPB decisions ordering the restoration of security clearances and the granting of access, the authority of the Secretary of the Navy to determine who will have access to classified information he is charged with protecting would be seriously impaired. Accordingly, Navy has petitioned for and is awaiting full MSPB review of the decisions of MSPB presiding officials who have improperly assumed this authority.

In the 30 years since the issuance of Executive Order 10450, the distinction between the standard of review which should be applicable to personnel security adjudication determinations and that actually applied to Federal employment suitability determinations has become blurred. The effect of this blurring has been the improper application of Federal employment suitability determination standards of review to personnel security adjudication questions, and, in turn, the failure to give proper weight and effect to behavior which may properly result in denial/revocation of security clearance and access. Determinations of trustworthiness consistent with the interests of national security require application of a standard of review more stringent than that applied to Federal employment suitability determinations.

In summary, we have an effective personnel security program, within the constraints of our ability to predict behavior and our investigative resources. We find that those personnel to whom we grant access to classified information are deserving of the trust we place in them, with only rare exceptions. Further refinements of the investigative and adjudicative process would give us better protection against the rare exceptions.

STATEMENT OF

UNITED STATES DEPARTMENT OF STATE

BEFORE THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

AT HEARINGS ON

U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM

APRIL 1985

U. S. DEPARTMENT OF STATE
PERSONNEL SECURITY PROGRAM

General Overview

The Department of State has 9,653 Foreign Service employees and 5,645 Civil Service employees. All of the Foreign Service employees occupy Critical Sensitive positions. Of the Civil Service employees, 4,304 occupy Critical Sensitive positions and the remaining 1,341 employees occupy Non-Sensitive positions. Of the total number of employees occupying Critical Sensitive positions, approximately 6,189 have SCI access.

For operational reasons, the Department no longer designates any positions Non-Critical Sensitive, other than some (approximately 100) associated with temporary appointments, such as internships and summer programs. Previously, a relatively small number of the Civil Service support positions located within the Main State building were designated Non Critical Sensitive. However, this was found to be inefficient. Since the majority of the positions within the Department are Critical Sensitive, those individuals occupying the Non Critical Sensitive positions would move to Critical Sensitive positions through the merit promotion process. This meant that usually within one or two years the investigation had to be reopened and expanded to a full field. In the end, this was a more costly process and, in many cases, information was developed during the full field investigation which if available at the time of the initial consideration, would have barred employment.

Non-Sensitive positions in the Department are physically located in annexes and include such functions as language instructors, warehousemen, employees of field Dispatch and Passport Agencies, etc.

Access

Employees occupying Critical Sensitive positions have access to classified information up to and including Top Secret on a strict need-to-know basis. These employees are issued a full access E.O. 10450 clearance, but in practice their access to National Security information will vary considerably depending on the position that they may occupy at any one time. This arrangement is needed to accommodate the assignment system within the Foreign Service. Employees normally serve two to three year tours of duty in one position or location and are then transferred. In this work environment, an employee may have little or no access in one assignment, but full access in his/her next assignment.

Background Investigations

Traditionally, the Department relied fully upon its own resources, Special Agents of the Office of Security, to conduct all of its background investigations. Because of manpower restraints resulting primarily from higher priority work, three years ago the Department began referring a significant amount of the investigations to OPM. When OPM's time service continued to deteriorate to the point at which it was taking five to six months to complete the investigations, the Department began to seek an alternate resource to conduct these investigations.

Because of OPM's heavy workload and time service problems, the Department stopped referring cases to OPM one year ago. To supplement its own resources, the Department now utilizes a cadre of approximately 140 contract investigators who are retired federal investigators, and, for the most part, retired FBI agents. The Department has individual contracts with these investigators, and these contracts were let through the competitive bidding process. The contracts are widely distributed (by design) throughout the United States and come under the operational control of the Department's nine domestic Security Field Offices.

As the result of its contract investigator program, the Department is now able to complete most of its full field background investigations in approximately 60 days. In that the Department found that in most instances it was able to complete the field investigations before OPM could complete the National Agency Check (NAC), it (the Department) now conducts its own NACs.

Although we do not yet have any final cost data, the Department estimates that a full field completed by a contractor is in the $900 range compared to OPM's cost of $1600 to $1700 (OPM charged the Department $100 extra to conduct our required personal interview). It should be noted that the average daily rate being paid the contractors is at about the GS-12 level; however, contractors receive no annual or sick leave benefits, no contributions to retirement, no logistical support, no personnel support, no medical benefits, etc.

For Critical Sensitive positions, the Department conducts a seven year full field background investigation. A traditional and highly valued portion of the Department's conducted background investigation is the personal interview of the applicant. Typically, the applicant is given a personal interview at the very beginning of the investigaton. During the interview, the investigator will question the applicant closely concerning his background and the data listed on his security forms. The applicant will be asked direct questions concerning such suitability/security issues as drugs, alcohol, finances, arrests, health, foreign associations, etc. The field investigation is then conducted to verify the information on the forms and statements made during the personal interview. If unexplained discrepancies develop as the result of the field investigation, a re-interview of the applicant will be scheduled.

The Department does not fill its Critical Sensitive positions prior to the completion of the full field background investigation. All security and suitability information developed during the background investigation is evaluated prior to any offer of employment. A total of 3,603 applicant investigations were completed during FY-80; 4,946 in FY-81; 3,937 in FY-82; 3,340 in FY-83; and, 3,385 in FY-84.

Adjudication and Due Process

The investigation results are processed by the Department's Division of Evaluations within the Office of Security. In that the security clearance criteria contained in E.O. 10450 parallels suitability standards, the Department, like most agencies, applies the investigative results to suitability standards and, therefore, essentially eliminates the need to make an adverse security clearance determination.

In the case of Foreign Service applicants, the investigative results are provided to a Foreign Service Final Review panel. That Panel, depending upon the type of Foreign Service candidate being considered, normally makes a final suitability decision based upon the results of the background investigation and on the results of oral and written examinations. Because of this process, it is difficult to determine which factor resulted in a non-selection -- the investigation, oral or written examinations, or a combination of all three. Traditionally, only one out of three applicants for the Foreign Service is successful.

In regard to Civil Service applicants, the investigative results, when deemed to be less than favorable, are forwarded to an Applicant Final Review Panel, comprised of members from Personnel, Medical, and the Office of Security. Based upon its review of the information, the Panel makes a suitability determination. During calendar year 1984, 83 cases were sent to the Panel and 54 were found to be unsuitable for employment.

Because of the above procedures, it is very rare that derogatory information in an appliant case has to be addressed from an aspect of security clearance. In the couple of isolated cases in recent years, both involved incumbents who occupied Non-Critical Sensitive or Non-Sensitive positions and sought merit promotions to Critical Sensitive positions. In these instances, the incumbent was informed of the reasons for the adverse decision and given the opportunity to respond to and appeal the decision.

Through procedures allowed in the Privacy Act of 1974, many unsuccessful applicants for employment have sought access to the investigative findings resulting in their non-selection. Generally, the Department has been successful in protecting the identity of confidential sources and that information (e.g., sole source information) which would be source revealing.

Reinvestigation/Reassessment

The Department complies with the reinvestigation criteria required of employees having SCI and other special access clearances (e.g., "Q," COSMIC, etc.). This includes the requirement that an update field investigation be conducted within the last five years. The Department utilizes its own investigative resources to conduct these investigations and averages around 300 investigations annually.

For incumbents of Critical Sensitive positions, the Department strives to meet the standards of E.O. 10450, requiring, on a five year cycle, the submission of an updated security questionnaire, review of the security and personnel files, and the conduct of a new National Agency Check. Because of past resource problems, there has been some slippage in this program. It is anticipated that this will be corrected within the next year.

Through the Department's network of Security Officers serving abroad at Embassies and in the Department, personnel security concerns are constantly addressed and monitored. For example, an employee arriving at an overseas post is given an arrival briefing by the Security Officer which addresses personnel security concerns such as travel restrictions, contact reporting requirements, the local hostile intelligence situation, etc. When that employee departs that post for an onward assignment, he is given a debriefing concerning all of the above and the personnel security situation that exists at that post as it may relate to other employees. In that the working/social environment at an overseas post is confined, this allows for developing personnel security problems to be readily identified and addressed.

The above security environment results in a flow of personnel security information and the initiation of "for cause" investigations as needed to resolve issues and allegations. In most instances, the issues are related to both security and personnel (suitability) concerns and are resolved administratively, either through separation or lesser disciplinary action.

Security concerns also play a role in the assignment process, in particular to those posts where hostile intelligence forces are active. In the interest of both the employee and the Department's personnel security program, employees who would be more vulnerable in this type of environment would not be favorably considered for such assignments. Typical areas of concern would be an unstable domestic situation, personal habits problems, atypical life styles, financial problems, relatives (native) living in the country, certain medical problems, etc.

Additional Comments

Like most agencies, the Department believes that E.O. 10450 is no longer a contemporary document upon which to build a viable personnel security program. A new Executive Order establishing a more specific security clearance criteria, would provide the Department with an alternate course of action to be taken in those instances when problem areas cannot be addressed as a personnel/suitability matter. It is to be noted that NSDD-84 directs that a new Executive Order be developed.

STATEMENT OF

DANIEL R. FOLEY

AND

JOHN R. HANCOCK

CO-CHAIRMEN

DOD INDUSTRIAL SECURITY REVIEW COMMITTEE

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

GOVERNMENT OPERATIONS COMMITTEE

UNITED STATES SENATE

APRIL 1985

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:

AS CO-CHAIRMEN OF THE DOD INDUSTRIAL SECURITY REVIEW COMMITTEE WE ARE PLEASED TO HAVE THE OPPORTUNITY TO PRESENT THIS PREPARED STATEMENT TO YOUR DISTINGUISHED BODY.

IN THE FALL OF 1983, IN THE WAKE OF THE JAMES D. HARPER, JR., ESPIONAGE CASE, GENERAL RICHARD G. STILWELL, THEN THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY, ESTABLISHED THE DOD INDUSTRIAL SECURITY REVIEW COMMITTEE. THE COMMITTEE WAS ASKED TO ANALYZE THE EFFECTIVENESS OF THE DEFENSE INDUSTRIAL SECURITY PROGRAM AND TO RECOMMEND NEEDED IMPROVEMENTS. THE COMMITTEE, WHICH WAS COMPRISED OF SIX REPRESENTATIVES OF SEVERAL DOD ELEMENTS AND ONE INDUSTRY ADVISOR, CONCLUDED ITS REVIEW IN NOVEMBER OF LAST YEAR AND ISSUED ITS FINAL REPORT TO GENERAL STILWELL THE FOLLOWING MONTH.

THE REPORT, ENTITLED "ANALYSIS OF THE EFFECTIVENESS OF THE DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY PROGRAM AND RECOMMENDATIONS FOR PROGRAM IMPROVEMENT", HAS BEEN PREVIOUSLY FURNISHED TO STAFF REPRESENTATIVES OF THIS SUBCOMMITTEE.

AS YOU KNOW, THE DEPARTMENT OF DEFENSE HAS DEVELOPED OVER THE YEARS A COMPREHENSIVE INDUSTRIAL SECURITY PROGRAM DESIGNED TO SAFEGUARD CLASSIFIED INFORMATION RELEASED TO INDUSTRY. THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY IS RESPONSIBLE FOR DEVELOPING AND APPROVING SECURITY POLICY UNDER THE DEFENSE INDUSTRIAL SECURITY PROGRAM (DISP). THE PROGRAM IS ADMINISTERED BY THE DIRECTOR, DEFENSE INVESTIGATIVE SERVICE (DIS). IT IS OUR UNDERSTANDING THE DIRECTOR, DIS, ALONG WITH REPRESENTATIVES FROM THE OFFICE OF THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY, MAY BE CALLED UPON DURING THESE PROCEEDINGS TO DISCUSS AND ANSWER QUESTIONS REGARDING INDUSTRIAL SECURITY POLICIES AND PRACTICES OF INTEREST TO THIS SUBCOMMITTEE. WE DESIRE, THEREFORE, TO LIMIT OUR COMMENTS TO THE FINDINGS OF THE REVIEW COMMITTEE WE JOINTLY CHAIRED.

THE DOD INDUSTRIAL SECURITY REVIEW COMMITTEE, OR "HARPER COMMITTEE" AS IT HAS BECOME POPULARLY KNOWN, DERIVED ITS CONCLUSIONS AND RECOMMENDED ACTIONS BASED ON CONTACT WITH HUNDREDS OF INDIVIDUALS THROUGHOUT GOVERNMENT AND INDUSTRY. OUR FINAL REPORT, WHICH IS FURNISHED FOR THE RECORD AS AN EXHIBIT TO THIS STATEMENT, INCLUDES 39 SEPARATE RECOMMENDATIONS. ABOUT 15 OF THESE RELATE GENERALLY TO PERSONNEL SECURITY, WHICH WE UNDERSTAND IS THE FOCAL POINT OF THESE HEARINGS, AND ONLY ABOUT ONE HALF OF THOSE PERTAIN TO PERSONNEL SECURITY CLEARANCE ASPECTS. THE INDUSTRIAL PERSONNEL SECURITY CLEARANCE PROGRAM IS OF VITAL IMPORTANCE BECAUSE IT IS CENTRAL TO THE ASSESSMENT PROCESS THAT ESTABLISHES ELIGIBILITY FOR CONTRACTOR EMPLOYEES TO HAVE ACCESS TO OUR NATIONAL SECURITY INFORMATION. ONLY THOSE INDIVIDUALS DETERMINED TO BE TRUSTWORTHY AND LOYAL ARE SECURITY CLEARED FOR ACCESS TO CLASSIFIED INFORMATION. A PERSONNEL SECURITY CLEARANCE CAN ONLY BE GRANTED OR CONTINUED WHEN IT IS DETERMINED TO BE CLEARLY CONSISTENT WITH THE NATIONAL INTEREST.

IT IS GENERALLY ACCEPTED THAT THE WEAKEST LINK IN THE SECURITY CHAIN IS THE CLEARED PERSONNEL HAVING ACCESS TO CLASSIFIED INFORMATION. HOSTILE INTELLIGENCE SERVICES HAVE LONG RECOGNIZED THAT IT IS LESS RISKY AND FAR MORE EFFECTIVE TO ENLIST THE SERVICES OF AN INDIVIDUAL ALREADY CLEARED THAN TO ATTEMPT PENETRATION OF A SECURITY SYSTEM THROUGH OTHER MEANS. A RESPONSIBLE AND CLEARED U.S. CITIZEN, ONCE COMPROMISED OR OTHERWISE INCLINED TO COMMIT AN ACT OF ESPIONAGE, CAN POTENTIALLY PROVIDE OUR ADVERSARIES WITH CLASSIFIED INFORMATION OVER A PERIOD OF MANY YEARS AND THUS CAUSE IRREPARABLE DAMAGE TO THE NATIONAL SECURITY.

IT REASONS, THEREFORE, THAT ALTHOUGH THE PERSONNEL SECURITY CLEARANCE PROGRAM IS BUT ONE ELEMENT IN A SECURITY SYSTEM OF SAFEGUARDS UNDER THE GENERAL SECURITY IN-DEPTH CONCEPT, IT PLAYS AN INTEGRAL PART OF THAT SYSTEM. IT IS ESSENTIAL THAT THE PROGRAM BE REVIEWED REGULARLY TO ASSURE OPTIMUM EFFICIENCY AND EFFECTIVENESS. INSOFAR AS OUR REVIEW COMMITTEE WAS ABLE TO DETERMINE, THE PROGRAM IS SUBJECTED TO REGULAR SCRUTINY. NONETHELESS, OUR RESEARCH DID UNCOVER OR RE-SURFACE CERTAIN SHORTCOMINGS WHERE IMPROVEMENT APPEARS CLEARLY WARRANTED. WE MUST EMPHASIZE THAT OUR EFFORT WAS NOT CONDUCTED ON A FULL-TIME BASIS, THE SCOPE OF OUR "CHARTER" WAS QUITE BROAD, AND IT SHOULD BY NO MEANS BE CONSIDERED A PERSONNEL SECURITY CLEARANCE PROGRAM REVIEW. OUR REVIEW DID, HOWEVER, RESULT IN THE IDENTIFICATION OF SEVERAL PERCEIVED WEAKNESSES OR SHORTCOMINGS. A FEW OF THE MORE RENOUNCED AREAS OF CONCERN AND OUR RECOMMENDED SOLUTIONS TO EACH ARE AS FOLLOWS:

1. SECRET CLEARANCES - THERE ARE APPROXIMATELY 1.4 MILLION CONTRACTOR EMPLOYEES CLEARED UNDER THE DISP. OF THIS TOTAL, OVER 900,000 ARE CLEARED AT THE SECRET LEVEL. THE REVIEW COMMITTEE CONSIDERED THE POLICY CONCERNING THE GRANTING OF SECRET CLEARANCES TO BE AMONG THE WEAKEST ASPECTS OF THE DOD PERSONNEL SECURITY CLEARANCE PROGRAM. UNDER NORMAL CIRCUMSTANCES, A SECRET CLEARANCE IS BASED ON A NATIONAL AGENCY CHECK (NAC) ALONE WITH NO PERIODIC UPDATE WHATSOEVER. THE REVIEW COMMITTEE CONSIDERED THE NAC TO BE AN INSUFFICIENT INVESTIGATIVE BASIS FOR ACCESS TO SECRET LEVEL NATIONAL SECURITY INFORMATION. HOWEVER, WE DID NOT FAVOR ABANDONING THE NAC, BUT RATHER SUPPLEMENTING IT WITH ADDITIONAL PRODUCTIVE SOURCES OF INVESTIGATIVE COVERAGE. WE RECOMMENDED SPECIFICALLY THAT THE NAC BE COMPLEMENTED BY A LOCAL AGENCY CHECK, CREDIT CHECK, AND EMPLOYMENT CHECK PRIOR TO THE GRANTING OF A FINAL SECRET CLEARANCE. WE ALSO RECOMMENDED THAT A REINVESTIGATION

BASED ON THE AFOREMENTIONED ENHANCED INVESTIGATIVE COVERAGE BE CONDUCTED AT 5-YEAR INTERVALS. THE PREVAILING THOUGHT IS THAT PERSONNEL SECURITY RISKS COMMENCE AFTER A CLEARANCE IS GRANTED AND INCREASE SIGNIFICANTLY THEREAFTER. WE ESTIMATE THAT THERE ARE LITERALLY THOUSANDS OF SECRET CLEARED INDUSTRIAL PERSONNEL HAVING ACCESS TO SECRET INFORMATION BASED ON A SIMPLE NAC CONDUCTED MORE THAN 20 YEARS AGO.

2. INTERIM CLEARANCE PROCEDURES - AS AN EMERGENCY MEASURE AND TO AVOID CRITICAL DELAYS IN PRE-CONTRACT NEGOTIATIONS OR CONTRACT PERFORMANCE, THE DOD PERMITS ISSUANCE OF A PERSONNEL SECURITY CLEARANCE BASED ON A LESSOR INITIAL INVESTIGATIVE COVERAGE THAN WOULD NORMALLY BE REQUIRED. THIS PROCEDURE IS DESIGNED TO AFFORD KEY INDUSTRIAL PERSONNEL ACCESS TO CLASSIFIED INFORMATION AT THE TIME SUCH CRITICAL ACCESS IS NEEDED WITHOUT HAVING TO AWAIT THE OUTCOME OF THE FULL INVESTIGATION NORMALLY REQUIRED. IN ESSENCE, ONCE THE INITIAL STAGE OF A REQUIRED INVESTIGATION IS COMPLETED, THE SUBJECT WILL BE GRANTED AN INTERIM CLEARANCE IF JUSTIFIED BY THE U.S. GOVERNMENT PROCUREMENT ACTIVITY AND THAT CLEARANCE WILL REMAIN VALID UNTIL SUCH TIME AS THE FULL INVESTIGATIVE EFFORT IS COMPLETED. ONCE COMPLETED, THE SUBJECT'S INTERIM CLEARANCE IS CONVERTED TO A FINAL CLEARANCE.

RECORDS INDICATE THAT FROM FY 1978 THROUGH FY 1984, THE DIS GRANTED: 76,545 INTERIM PERSONNEL SECURITY CLEARANCES; 2,231 TOP SECRET; 73,539 SECRET; AND 775 CONFIDENTIAL. OVER 13,000 INTERIM CLEARANCES WERE GRANTED BY THE DIS IN FY 1984 ALONE WHICH REPRESENTS 5 PERCENT OF THE TOTAL INDUSTRIAL CLEARANCES ISSUED. GIVEN THAT ISSUANCE OF INTERIM CLEARANCES HAS NOT PROVEN UNDULY RISKY AND THEY CAN BE TIMELY GRANTED NORMALLY BETWEEN 1 TO 30 DAYS DEPENDING ON THE LEVEL OF CLEARANCE REQUESTED, THE REVIEW COMMITTEE RECOMMENDED THAT THE INTERIM CLEARANCE CONCEPT BE ADOPTED FOR GENERAL USE SYSTEM-WIDE.

ADOPTION OF THE INTERIM SYSTEM WOULD REDUCE THE AVERAGE TIME BETWEEN RECEIPT OF A CLEARANCE APPLICATION BY THE DIS AND THE ISSUANCE OF THE CLEARANCE TO MUCH LESS THAN 30 DAYS FOR A SECRET LEVEL CLEARANCE. INDUSTRY CANNOT AFFORD TO HAVE ITS EMPLOYEES IDLE FOR MONTHS, OR TO PLACE EMPLOYEES IN A TEMPORARY OR LESS SENSITIVE POSITION, WHILE THEY AWAIT THE GRANTING OF THEIR CLEARANCES AS THE PRESENT SYSTEM DICTATES.

A MAJOR 1982 REVIEW OF THE DOD PERSONNEL SECURITY PROGRAM CONFIRMED THE DELETERIOUS EFFECTS OF THE EXCESSIVE TIME LAG EXPERIENCED IN RECEIVING THE RESULTS OF A DIS INVESTIGATION. THAT REVIEW DID NOT, HOWEVER, ADDRESS THE PARALLEL AND POTENTIALLY MORE DAMAGING EFFECTS INCURRED BY INDUSTRY FROM SUCH TIME LAGS. THESE EXCESSIVE TIME LAGS ACTUALLY ENCOURAGED CONTRACTORS TO REQUEST CLEARANCES FOR THEIR EMPLOYEES AT THE HIGHEST CONCEIVABLE LEVEL EVEN THOUGH IMMEDIATE OR NEAR-TERM ACCESS TO CLASSIFIED INFORMATION IS NOT REQUIRED. THEY DO THIS TO AVOID UNACCEPTABLE LENGTHY CLEARANCE PROCESSING TIMES. WHEN CONTRACTORS HAVE A CLEAR NEED TO FURNISH EMPLOYEES CLASSIFIED INFORMATION, THEY CANNOT WAIT MONTHS FOR THEM TO BE SECURITY CLEARED. UNTIL THE PROCESSING TIME LEADING UP TO THE ISSUANCE OF A PERSONNEL SECURITY CLEARANCE CAN BE SIGNIFICANTLY REDUCED, MANY CONTRACTORS WILL CONTINUE TO USE THE "SHOTGUN" APPROACH TO REQUESTING CLEARANCES.

SUCH PRACTICES DRIVE UP CONTRACT COSTS AND ENCUMBER DEFENSE PRODUCTION. THE EXTENSION OF INTERIM INVESTIGATIVE PROCEDURES ALREADY IN USE BY THE DOD WOULD NOT REDUCE FULL INVESTIGATIVE COVERAGE BUT WOULD PERMIT "CLEAN" CASES TO BE GRANTED CLEARANCES EARLY ON DURING THE INVESTIGATIVE PROCESS BASED ON THE PROJECTION THAT A CLEARANCE WOULD LIKELY BE GRANTED ANYWAY. IN OUR VIEW, AN INTERIM TYPE SYSTEM SHOULD BE PLACED INTO EFFECT AT THE EARLIEST PRACTICAL TIME FOR ALL THREE LEVELS OF CLEARANCE, ESPECIALLY TOP SECRET, IN ORDER TO CONTRIBUTE SIGNIFICANTLY TO A REDUCTION IN CLEARANCE REQUESTS AND TO ASSIST

IN THE ON-GOING NATIONAL CONCERN TO REDUCE THE COSTS ASSOCIATED WITH DEFENSE PRODUCTION SO FREQUENTLY MENTIONED BY THE PRESS.

3. PERIODIC REINVESTIGATIONS - 5-YEAR PERIODIC REINVESTIGATIONS (PR'S) ARE REQUIRED TO BE CONDUCTED FOR ALL TOP SECRET CLEARED PERSONNEL AS WELL AS THOSE CLEARED FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI). THE REVIEW COMMITTEE CONSIDERS THE CONDUCT OF PR'S TO BE VITAL AND SUBSTANTIALLY MORE IMPORTANT THAN THE ORIGINAL INVESTIGATION. NONETHELESS, ONLY ABOUT 47,000 PR'S HAVE BEEN CONDUCTED SINCE APRIL OF 1983 DESPITE THE FACT THAT THE NUMBER OF PERSONS DOD-WIDE WHO NOW MEET THE 5-YEAR REINVESTIGATION CRITERIA STANDS AT 279,000. BASED ON PROJECTED INCREASES, DIS WOULD HAVE TO COMPLETE ABOUT 115,000 PR'S ANNUALLY FOR 5 YEARS TO SATISFY ITS PR WORKLOAD. HOWEVER, GIVEN EXISTING RESOURCES, IT DOES NOT APPEAR THAT THE DIS WOULD EVEN COME CLOSE TO COMPLETING SUCH A HEAVY PR WORKLOAD. DURING FY 1984, FOR EXAMPLE, THE DIS WAS ABLE TO COMPLETE ONLY 32,000 PR'S.

THE DOD CURRENTLY USES A QUOTA SYSTEM IN THE ADMINISTRATION OF THE PR PROGRAM BECAUSE THE EXISTING AND PROJECTED PR WORKLOAD CANNOT BE ACCOMPLISHED BY THE DIS WITH EXISTING RESOURCES. THE SYSTEM ESSENTIALLY CONSISTS OF CONDUCTING THE OLDEST CASES FIRST. HOWEVER, CONTRARY TO THE VIEW OF SOME DOD OFFICIALS WHO ADVOCATE RESOLUTION OF THE PR PROBLEM BY A MASSIVE INFUSION OF ADDITIONAL MANPOWER, THE REVIEW COMMITTEE RECOMMENDED CONSIDERATION OF AN ALTERNATIVE APPROACH.

PERIODIC REINVESTIGATIONS ARE IMPORTANT BECAUSE PERSONS SUBJECT TO THEM ARE ASSUMED TO BE HAVING ACCESS TO SOME OF OUR MOST SENSITIVE INFORMATION, THAT IS TOP SECRET AND SCI INFORMATION. HOWEVER, IT IS GENERALLY ACCEPTED THAT A LARGE NUMBER OF PERSONNEL SUBJECT TO A PR ARE NOT IN FACT HAVING SUCH SENSITIVE ACCESS. AS CONCERNS THE ROUGHLY 115,000 INDUSTRIAL EMPLOYEES CLEARED AT THE TOP SECRET LEVEL, THE COMMITTEE ESTIMATED THAT PERHAPS 90,000

TO 95,000 OF THEM DO NOT HAVE CONTINUOUS OR EVEN FREQUENT ACCESS TO TOP SECRET INFORMATION AND PROBABLY NO MORE THAN 35,000 TO 40,000 OF THEM HAVE EVER HAD ACCESS TO TOP SECRET INFORMATION.

LOGICALLY SPEAKING, THEREFORE, ONLY EMPLOYEES WHO ACTUALLY HAVE ACCESS TO TOP SECRET AND SCI SHOULD BE SUBJECT TO A PR. THE DOD CAN ILL-AFFORD TO EXPEND ITS LIMITED INVESTIGATIVE RESOURCES CONDUCTING PR'S SIMPLY BECAUSE SOMEONE IS CLEARED TOP SECRET OR IS LISTED ON AN SCI ACCESS LIST. THE REVIEW COMMITTEE RECOMMENDED THEREFORE THAT PR'S NOT BE CONDUCTED ON PERSONNEL WHO HAVE ONLY OCCASIONAL ACCESS TO TOP SECRET OR SCI, HAVE NOT HAD SUCH ACCESS FOR A CONSIDERABLE PERIOD OF TIME, OR WHO HAVE NEVER HAD ACCESS TO THIS SENSITIVE INFORMATION. THE SOLUTION THEREFORE, IS FOR THE DOD TO DEVELOP A SYSTEM TO DETERMINE WHO IS HAVING ACCESS TO CLASSIFIED INFORMATION AND TO WHAT EXTENT AND LEVEL. WE BELIEVE THAT ONCE THIS IS ACCOMPLISHED, THE DIS PR WORKLOAD WILL BE REDUCED SUBSTANTIALLY. IT WOULD CERTAINLY ELIMINATE THE CONDUCT OF PR'S ON PERSONS WHO DON'T NEED THEM. IT WOULD ALSO SINGLE OUT THOSE WHO DO.

4. ONE-TIME ACCESS - FROM FY 1981 THROUGH FY 1984 THE NUMBER OF DOD PERSONNEL SECURITY CLEARANCES GRANTED TO INDUSTRIAL PERSONNEL INCREASED APPROXIMATELY 50 PERCENT. THE DIS ISSUED OVER 257,000 CLEARANCES IN FY 1984 ALONE. IN MARCH 1984, THE DIS COMPONENT RESPONSIBLE FOR PROCESSING PERSONNEL SECURITY CLEARANCE REQUESTS RECEIVED NEARLY 26,000 CLEARANCE APPLICATIONS, THE LARGEST MONTHLY FIGURE EVER RECORDED. IN SHORT, THE DOD INDUSTRIAL SECURITY PROGRAM IS IN THE MIDST OF AN UNPRECEDENTED PROLIFERATION OF PERSONNEL SECURITY CLEARANCE ACTIONS.

BECAUSE OF THE UNACCEPTABLE CLEARANCE PROCESSING TIMES INVOLVED, MANY CONTRACTORS TEND TO REQUEST PERSONNEL SECURITY CLEARANCES ON BEHALF OF THEIR EMPLOYEES IN NUMBERS AND AT CLASSIFICATION LEVELS BEYOND ANY KNOWN IMMEDIATE

OR PROJECTED NEED. THIS ABUSE OF THE SYSTEM, AND IT IS AN ABUSE, ENABLES INDUSTRY TO AVOID AWAITING THE OUTCOME OF LENGTHY INVESTIGATIONS. FOR EXAMPLE, INDUSTRY ON OCCASION WILL REQUEST A TOP SECRET CLEARANCE FOR A PARTICULAR EMPLOYEE AS A CONTINGENCY MEASURE. THIS WILL ASSURE THAT SHOULD THAT EMPLOYEE EVER HAVE A NEED, EVEN A ONE-TIME NEED, TO SEE A TOP SECRET DOCUMENT, THE EMPLOYEE WILL ALREADY HAVE BEEN GRANTED THE HIGHER LEVEL CLEARANCE AND ACCESS CAN BE AFFORDED TO THAT INDIVIDUAL IMMEDIATELY. TO OVERCOME THIS PROPENSITY TO CLEAR EMPLOYEES BEYOND A CLEARLY ESTABLISHED LEVEL OF NEED, AND TO REDUCE COSTLY AND UNNECESSARY INVESTIGATIONS, THE REVIEW COMMITTEE RECOMMENDED THAT GREATER FLEXIBILITY BE BROUGHT INTO THE SYSTEM. MORE SPECIFICALLY, WE RECOMMEND THAT UNDER JUSTIFIABLE CIRCUMSTANCES, THE DIS SHOULD BE AUTHORIZED TO APPROVE CONTRACTOR EMPLOYEES FOR ACCESS BEYOND THE LEVEL OF THEIR RESPECTIVE PERSONNEL SECURITY CLEARANCES. THE PROCEDURE WOULD BE LIMITED TO EMPLOYEES ALREADY INVESTIGATED BY THE DOD WHO POSSESS CURRENT CLEARANCES. IN ADDITION, IT WOULD ONLY BE USED TO FACILITATE UNFORESEEN CIRCUMSTANCES WHICH REQUIRE A PARTICULAR EMPLOYEE TO SEE HIGHER LEVEL CLASSIFIED INFORMATION ON A ONE-TIME OR OCCASIONAL BASIS. SHOULD RECURRING ACCESS TO HIGHER LEVEL INFORMATION BE REQUIRED, THE REQUISITE INVESTIGATION WOULD, OF COURSE, BE CONDUCTED AS USUAL.

QUITE FRANKLY, IT DOES NOT APPEAR WARRANTED FOR THE DOD TO CONTINUE TO INCURE THE COST OF EXPENSIVE INVESTIGATIONS IN CASES WHERE THE NEED FOR ACCESS TO HIGHER LEVEL CLASSIFIED INFORMATION IS REMOTE OR, AT MOST, IS ONLY REQURIED ON A SINGLE OCCASION OR PERHAPS TWO OR THREE OCCASIONS OVER A PERIOD OF MANY YEARS.

5. CLEARANCE JUSTIFICATION AND ADMINISTRATIVE DOWNGRADES - DOD POLICY REQUIRES CONTRACTORS TO REVIEW THE ACCESS AFFORDED TO TOP SECRET

CLEARED PERSONNEL. WHEN SUCH PERSONNEL HAVE NOT HAD ACCESS TO TOP SECRET INFORMATION DURING THE PRECEDING 18-MONTH PERIOD AND ACCESS AT THAT LEVEL IS NOT ANTICIPATED IN THE FORESEEABLE FUTURE, INDUSTRY IS REQUIRED TO INITIATE ADMINISTRATIVE DOWNGRADING ACTION. SUCH ADMINISTRATIVE DOWNGRADING PROVISIONS ARE ONLY VOLUNTARY FOR SECRET LEVEL CLEARANCES RESULTING IN ONLY A RELATIVELY FEW CLEARANCES ADMINISTRATIVELY DOWNGRADED TO THE NEXT LOWER LEVEL OF CLASSIFICATION IN THIS MANNER. BY ANY ACCOUNT, MANY PERSONNEL SECURITY CLEARANCES THAT CAN NO LONGER BE SUPPORTED, OR ARE NO LONGER NEEDED AT THE HIGHER LEVEL, ESCAPE DOWNGRADE OR TERMINATION ACTION. COMPLIANCE IS, THEREFORE, RATHER SPOTTY AND THE BULK OF CONTRACTOR CLEARANCES REQUIRING SUCH ACTION REMAIN IN EFFECT YEAR AFTER YEAR. THE EXISTENCE OF PERSONNEL CLEARANCES THAT CAN NO LONGER BE JUSTIFIED CONTRIBUTES TO THE CONDUCT OF MANY UNNECESSARY CLEARANCE ACTIONS.

THE REVIEW COMMITTEE RECOMMENDED ADOPTION OF AN AFFIRMATIVE SYSTEM, EXPANDED TO INCLUDE SECRET CLEARANCES, THAT WOULD REQUIRE CONTRACTORS TO JUSTIFY EXISTING CLEARANCES TO THE DIS AT 5-YEAR INTERVALS. IF RETENTION OF AN EXISTING CLEARANCE AT A PARTICULAR CLASSIFICATION LEVEL CANNOT BE JUSTIFIED, THAT CLEARANCE WOULD BE ROUTINELY DOWNGRADED TO THE NEXT LOWER LEVEL. IN OTHER WORDS, EVIDENCE TO SUPPORT CONTINUATION OF PERSONNEL SECURITY CLEARANCES AT THE TOP SECRET AND SECRET LEVEL WOULD BE REQUIRED, IN EACH INSTANCE, BOTH INITIALLY AND PERIODICALLY.

IN THIS CONNECTION, THE REVIEW COMMITTEE RECOMMENDED USE OF A CLEARANCE JUSTIFICATION DATA SHEET TO BE COMPLETED BY INDUSTRY AND FURNISHED TO THE DIS. THIS DATA SHEET, THE SUBSTANCE OF WHICH COULD EVENTUALLY BE INCORPORATED INTO STANDARD DOD CLEARANCE APPLICATION FORMS, WOULD CONTAIN THE FOLLOWING INFORMATION:

- CLEARANCE APPLICANT OR CLEARED EMPLOYEE CERTIFICATION THAT HIS OR HER DUTIES AND RESPONSIBILITIES OF THE CURRENT POSITION REQUIRE ACCESS TO CLASSIFIED INFORMATION AT A PARTICULAR LEVEL;
- IMMEDIATE SUPERVISOR CERTIFICATION THAT THE CLEARANCE APPLICANT OR CLEARED EMPLOYEE OCCUPIES A POSITION THAT REQUIRES ACCESS TO CLASSIFIED INFORMATION AT A PARTICULAR LEVEL;
- CONFIRMATION BY A TOP MANAGEMENT OFFICIAL OF THE FIRM THAT THE INITIAL CLEARANCE OR CONTINUATION REQUEST HAS BEEN REVIEWED AND THAT THE CLEARANCE IS FULLY JUSTIFIED.

THE REVIEW COMMITTEE PROPOSAL WOULD INCLUDE ALL THREE OF THE AFOREMENTIONED PERSONS IN EACH CLEARANCE ACTION, TO INCLUDE ANY PERIODIC UPDATES, AND WOULD ADVISE THE CERTIFYING INDIVIDUALS OF THE CONSEQUENCES OF WILLFULLY OR FALSELY SUPPORTING THE NEED FOR AN UNNECESSARY PERSONNEL SECURITY CLEARANCE.

IN SUMMARY, THE DOD CAN NO LONGER AFFORD TO PROCESS CLEARANCES ON BEHALF OF PERSONS WHO DO NOT NEED THEM. A SUBSTANTIAL NUMBER OF PERSONNEL SECURITY CLEARANCE ACTIONS ARE CONDUCTED WHEN ACCESS TO CLASSIFIED INFORMATION IS NOT REQUIRED AND A SUBSTANTIAL NUMBER OF CLEARANCES ALREADY GRANTED REMAIN IN PLACE WHEN ADMINISTRATIVE DOWNGRADING OR TERMINATION ACTION IS CALLED FOR.

THE REVIEW COMMITTEE FIRMLY BELIEVES THAT ADOPTION OF THE RECOMMENDATIONS JUST ENUMERATED WILL SAVE SUBSTANTIAL INVESTIGATIVE RESOURCES AND CONTRIBUTE SIGNIFICANTLY TO ENHANCE SECURITY OVERSIGHT. THE ONLY ALTERNATIVE, WHICH WE CONSIDER UNACCEPTABLE, IS TO CONTINUE DOING BUSINESS AS USUAL AND TO ALLOCATE EVER INCREASING FUNDS TO PAY FOR AN INVESTIGATIVE WORKLOAD THAT IS SOMEWHAT INFLATED UNDER THE PRESENT SYSTEM. WHILE ADOPTION OF SOME OF THE REVIEW COMMITTEE RECOMMENDATIONS MAY APPEAR COSTLY AND MANPOWER-INTENSIVE, OTHERS WILL RESULT IN SAVINGS IN COSTS AND LABOR. WE WOULD ALSO LIKE TO ADD THAT

FAR TOO MUCH RELIANCE IS PLACED ON THE EXISTENCE OF A PERSONNEL SECURITY CLEARANCE. AS MEMBERS OF THIS SUBCOMMITTEE WELL KNOW, THE MORE IMPORTANT CRITERION FOR ACCESS TO CLASSIFIED INFORMATION IS ESTABLISHMENT OF A CLEAR-CUT NEED-TO-KNOW FOR ACCESS TO THE SPECIFIC INFORMATION INVOLVED. UNFORTUNATLEY, TOO LITTLE EMPHASIS IS NOW PLACED ON THE NEED-TO-KNOW ACCESS PREREQUISITE. OUR COMMITTEE ALSO REVIEWED PHYSICAL SECURITY ASPECTS OF THE INDUSTRIAL SECURITY PROGRAM. IN THIS CONNECTION, WE HAVE RECOMMENDED SEVERAL COURSES OF ACTION DESIGNED TO MAKE IT SIGNIFICANTLY MORE DIFFICULT FOR UNSCRUPULOUS OR CARELESS INDUSTRIAL EMPLOYEES TO REMOVE CLASSIFIED MATERIAL FROM THE PREMISES OF CLEARED CONTRACTOR FACILITIES.

STATEMENT OF

STEVEN GARFINKEL
DIRECTOR
INFORMATION SECURITY OVERSIGHT OFFICE (ISOO)
GENERAL SERVICES ADMINISTRATION

BEFORE THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

AT HEARINGS ON

U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM

APRIL 1985

THE INFORMATION SECURITY OVERSIGHT OFFICE

Background

Government secrecy is as old as government itself. Government secrecy in an information society, however, is a new phenomenon. In balancing the needs of national security with the commitment of access to information, the executive branch of the United States Government confronts a challenge that no other national government, past or present, has faced. The security side of the equation is the Government-wide information security system.

The information security system comprises the body of rules and procedures for classifying, declassifying and safeguarding national security information. These rules and procedures, currently embodied in Executive Order 12356, apply to all executive branch agencies, their contractors, licensees and grantees that generate or handle national security information. The system's purpose is to identify and limit access to that body of information that requires protection in the interest of national security.

President Reagan signed Executive Order 12356 on April 2, 1982. It is the fifth Executive order on national security information since World War II. Each Administration has defended the use of the Executive order for this purpose on the basis that the information security system represents the exercise of presidential prerogatives under the Constitution. There have been a number of bills introduced as substitutes over the years, but the Congress has never enacted one.

For the information security system to function properly, the executive branch must attempt to classify and protect only that very small portion of information that requires it in the interest of the national defense or foreign relations. Often, decisions about what, how much, and how long to classify are not easy; sometimes they are susceptible to abuse. The system requires controls.

That the information security system is under control results from several factors. One of the most important is the high degree of oversight, or monitorship, that the program receives. E.O. 12356 mandates oversight from two sources: First, each agency head must administer "an active oversight and security education program;" and second, the Information Security Oversight Office "shall oversee agency actions to ensure compliance with [the] Order and [its] implementing directives."

In a larger sense, of course, oversight also flows from outside the executive branch of Government: For example, from the continuing interest of various committees, subcommittees and individual members of Congress; from the constant media attention and criticism; and from the historians, students, researchers and other individuals whose inquiries and requests, and sometimes whose lawsuits, prompt intense scrutiny of individual classification decisions. While all of these contribute to successful oversight, this paper examines the role of the centralized oversight entity, the Information Security Oversight Office, or ISOO.

Overseeing the Information Security Program

Established by Executive Order 12065 on December 1, 1978, ISOO operates now under the provisions of Executive Order 12356, effective August 1, 1982. ISOO is responsible for overseeing the information security programs of all executive branch activities that create or handle national security information. E.O. 12356 also requires the Director of ISOO to report annually to the President on the progress of executive branch agencies in implementing the Order's provisions. In monitoring the program, ISOO oversees the information security programs of approximately 65 departments and independent agencies or offices of the executive branch.

ISOO is located administratively in the General Services Administration but receives its policy direction from the National Security Council. The Administrator of General Services appoints the ISOO Director upon approval of the President. The ISOO Director appoints the staff, which numbers between 13-15 persons. For FY 1985, ISOO budget is $662,000.

The information security program worldwide involves tens of thousands of facilities, millions of people, and hundreds of millions of dollars. That an office of ISOO's size cannot oversee the entire program itself is self-evident. Therefore, ISOO's primary function is to oversee the overseers; i.e., ISOO's job is to assure itself that the agencies are adequately overseeing their own internal and contractual programs. To accomplish this function, the President in E.O. 12356 has assigned the Director of ISOO a large number of authorities and responsibilities for the program.* These may be conveniently grouped into the following categories: (a) Developing and issuing implementing directives and instructions regarding the Order; (b) conducting on-site inspections or program reviews of monitored agencies; (c) gathering, analyzing and reporting statistical data on agencies' programs; (d) evaluating, developing or disseminating security education materials and programs; (e) receiving and taking action on suggestions, complaints, disputes and appeals from persons inside or outside the Government on any aspect of the administration of the Order; and (f) conducting special studies on problem areas or programs to improve the system.

---

* Under E.O. 12356, the Director of ISOO's specific program authorities and responsibilities include:

(a) developing and promulgating directives implementing the Order (Sec. 5.2(b)(1));
(b) overseeing agency actions (Sec. 5.2(b)(2));

Like most oversight organizations, ISOO is more closely associated with program reviews or inspections of other agencies than with any other activity. To carry out this function, ISOO maintains a liaison system in which each agency that creates or handles national security information has an assigned ISOO analyst. This analyst is responsible both for conducting formal program reviews and inspections, and for maintaining an informal dialogue throughout the year in response to questions or problems.

At least once a year, the ISOO analyst conducts a formal inspection of each of his or her assigned agencies. These on-site inspections encompass all aspects of the information security program, including classification, declassification, safeguarding, security education and training, and administration. The inspections always include detailed interviews with agency security personnel, classifiers, and handlers of national security information. To the maximum extent possible, ISOO analysts review a sampling of classified information in the agency's inventory to examine the propriety of classification, the existence of necessary security markings and instructions, and compliance with safeguarding procedures. ISOO analysts also monitor security education and training programs to determine if they adequately inform appropriate personnel about classifying, declassifying, marking, and safeguarding national security information. When deficiencies in an agency's program are noted, ISOO analysts recommend corrections, either on-the-spot or as part of a formal inspection report. Critical reports require immediate remedial attention by the agency prior to a follow-up inspection by ISOO. These inspections are a necessary means of identifying and resolving problem areas. They provide positive indicators of agency compliance or non-compliance with the Executive order that are not apparent simply from the analysis of statistical data.

(c) reviewing agency regulations and systematic review guidelines (Sec. 5.2(b)(3));
(d) conducting on-site reviews of and requiring reports about agency programs (Sec. 5.2(b)(4));
(e) reviewing and recommending to the President additional requests for original classification authority (Sec. 5.2(b)(5));
(f) considering and taking action on complaints and suggestions (Sec. 5.2(b)(6));
(g) prescribing standard forms (Sec. 5.2(b)(7));
(h) reporting to the President (Sec. 5.2(b)'8));
(i) convening and chairing interagency meetings (Sec. 5.2(b)(9));
(j) receiving and forwarding to appropriate agencies information that may require classification (Sec. 1.2(e));
(k) receiving notification of other categories of information determined by agency heads to require classification (Sec. 1.3(a)(10));

Relationship to the Personnel Security Program

ISOO has no direct oversight authority for the personnel security program. However, no Federal security system operates in a vacuum. The programs overlap and interact. Section 4.1(a) of E.O. 12356 spells out the critical link between the information security system and the personnel security system: "A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes." The "determination of trustworthiness" is the clearance, a product of the personnel security system.

(l) receiving notification of portion marking waivers (Sec. 1.5(b));
(m) prescribing standard marking designations (Sec. 1.5(c));
(n) receiving notification of reclassification actions (Sec. 1.6(c));
(o) receiving notification of classification guide waivers (Sec. 2.2(c));
(p) requiring an agency to declassify information determined to be classified in violation of the Order (Sec. 3.1(c));
(q) issuing systematic review guidelines for foreign government information (Sec. 3.3(a));
(r) deciding mandatory review appeals regarding classified presidential papers or records (Sec. 3.4(b));
(s) having access to accountings of special access programs (Sec. 4.2(b));
(t) reporting violations to agencies (Sec. 5.4(a)); and
(u) receiving reports of unauthorized disclosures or unauthorized classification (Sec. 5.4(d)).

It is generally agreed that the number of national security clearances among executive branch employees far exceeds the number of employees who require access to classified information in order to perform their jobs. To ISOO's knowledge, the number difference is unknown. On occasion ISOO will discover in its inspections program a clear discrepancy between the classification activity within an agency and the approximate number of its cleared personnel. In its inspection report, ISOO will strongly recommend a review of the number of clearances. Unfortunately, these discrepancies are readily apparent only in agencies with very small classification programs. To discover these discrepancies in the agencies with significant classification programs would require resources far beyond ISOO's.

Standardized nondisclosure agreements provide another link between the personnel and information security systems. In compliance with National Security Decision Directive 84, "Safeguarding National Security Information," executed by the President in March 1983, ISOO issued the "Classified Information Nondisclosure Agreement," Standard Form 189. Ultimately, all persons whose jobs require national security information clearances, both within and outside Government, must sign the SF 189 as a condition of access to classified information. The only exceptions will be those persons who work for agencies that have received waivers because their personnel already sign nondisclosure agreements at least as stringent.

Conclusion

In a society that bombards itself with information, a Government system designed to prevent the public disclosure of certain information attracts constant scrutiny. Despite its critical importance to the nation, the information security system under every presidential administration since World War II has been subjected to criticism about its scope and purpose. With the onset of the Freedom of Information age, the tension between access to information and the protection of national security has increased.

The Information Security Oversight Office serves to help ease that tension. Through various oversight initiatives it strives to limit the extraordinary protection of national security classification to only that very sensitive information that merits such shelter. ISOO efforts, combined with those from many other sources, have resulted in an information security system that not only works, but works under control. In order to maintain that control, the scrutiny from within the system must continue to match the scrutiny from without. ISOO is pledged to meet that objective.

Appendix A .

ISOO INSPECTIONS - FY83/84

AGENCY FOR INTERNATIONAL DEVELOPMENT

- Bureau for Africa
- Bureau for Asia
- Office of Security

ARMS CONTROL AND DISARMAMENT AGENCY
- Office of Administration
  - Communications Section
- Strategic Programs Bureau
- General Advisory Commission on Arms Control
- Bureau of Multilateral Affairs

BOARD FOR INTERNATIONAL BROADCASTING

CENTRAL INTELLIGENCE AGENCY

- Directorate of Intelligence
- Directorate of Administration
- Directorate of Science and Technology
- Directorate of Operations
- Other Major Activities

CIVIL AERONAUTICS BOARD

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

DEFENSE COMMUNICATIONS AGENCY

DEFENSE CONTRACT AUDIT AGENCY

DEFENSE INTELLIGENCE AGENCY

- Directorate for Estimates
- Directorate for Scientific and Technical Intelligence
- Directorate for Intelligence and External Affairs
- Directorate for Communications
- Directorate for Foreign Intelligence
- Directorate for JCS Support
- Directorate for Research

DEFENSE INVESTIGATIVE SERVICE

DEFENSE LOGISTICS AGENCY

- Headquarters
- Defense Technical Information Center

DEFENSE MAPPING AGENCY

- Headquarters' Office of Security
- Office of Distribution Services
- Hydrographic/Topographic Center
- Special Security Office

DEFENSE NUCLEAR AGENCY

- Intelligence and Security Directorate
  - Counterintelligence Detachment
  - Classification Management Division
  - Security and Operations Division
- Radiation Directorate
- Shock Physics Directorate

DEPARTMENT OF AGRICULTURE

DEPARTMENT OF COMMERCE

- Headquarters' Office of Security
- National Telecommunications and Information Administration
- International Trade Administration

DEPARTMENT OF EDUCATION

DEPARTMENT OF HEALTH AND HUMAN SERVICES

- Office of the Secretary
- Food and Drug Administration
- National Institutes of Health

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

DEPARTMENT OF INTERIOR

- Headquarters' Office of Security
- U. S. Geological Survey
- Bureau of Mines

DEPARTMENT OF JUSTICE

- Federal Bureau of Investigation
- Immigration and Naturalization Service
- Drug Enforcement Administration
  - El Paso Intelligence Center
- Bureau of Prisons
- Foreign Claims Settlement Commission
- Main Justice
  - Antitrust Division
  - Civil Division
  - Criminal Division
  - Tax Division
  - Bureau of Prisons
  - Foreign Claims Settlement Commission
  - Justice Management Division
  - Office of Intelligence Policy and Review
  - Office of Information and Privacy
  - Antitrust Division

DEPARTMENT OF LABOR

- Office of Emergency Preparedness Planning (Information Security)
- Bureau of International Labor Affairs
- Bureau of Labor Management Relations and Corporate Programs

DEPARTMENT OF STATE

- Classification/Declassification Center
- Information Systems Office
- Information Systems Security Staff
- Office of Security
  - Domestic Operations
  - Education and Training Staff
- Bureau of Intelligence and Research
  - Office of the Executive Director
  - Office of Economic Analysis
- Bureau of East Asian and Pacific Affairs: Japan

- United States Mission to the United Nations
  - Office of Administrative Affairs
    - Reference Section
  - Political Section
  - Economic and Social Section
  - Communications Section
  - Security
  - Resources Management

DEPARTMENT OF THE AIR FORCE

- Assistant Chief of Staff, Intelligence
- Assistant Chief of Staff, Information Systems
- Deputy Chief of Staff, Plans and Programs
- Deputy Chief of Staff, Research, Development and Acquisition
- Deputy Chief of Staff, Programs and Resources
- 1947 Headquarters Support Group - Air Staff
- Air Force Systems Command (Andrews Air Force Base)
    - Electronics Systems Division (Hanscom Air Force Base)
    - Aerospace Systems Division (Wright-Patterson AFB)
    - Foreign Technology Division (Wright-Patterson AFB)
- Air Force Logistics Command Headquarters (Wright-Patterson AFB)

DEPARTMENT OF THE ARMY

- Assistant Chief of Staff for Intelligence
- Deputy Chief of Staff for Operations
- Military District of Washington
- Criminal Investigation Command
- Comptroller of the Army
- Logistical Command
- Military Traffic Management Command
- Surgeon General
- Research Development and Acquisition
- Office of the Adjutant General
- National Guard Bureau
- Intelligence and Security Command
- Corps of Engineers
- Materiel Development and Readiness Command
- Missile Intelligence Agency, Huntsville, Ala.
- Ballistic Missile Defense Systems Command, Huntsville, Ala.
- U. S. Army Missile Command, Huntsville, Ala.
- Communications - Electronics Command, Ft. Monmouth, N.J.
- U. S. Army Natick Research and Development Command, Natick, Mass.
- Army Materials and Mechanics Research Center, Watertown, Mass.
- White Sands Missile Range, Las Cruces, New Mexico

DEPARTMENT OF THE NAVY

- Office of the Chief of Naval Operations
- Naval War College, Newport, R.I.
- Naval Underwater Systems Center, Newport, R.I.
- Naval Underwater Systems Center, New London, Cn.
- Naval Intelligence Support Center
- Naval Research Laboratory
- Joint Cruise Missile Project Office
- Office of Command Control
- U.S. Atlantic Fleet Headquarters, Norfolk, Va.
- Commander Naval Surface, U.S. Atlantic Fleet, Norfolk, Va.
- Headquarters Fleet Marine Force Atlantic, Norfolk, Va.
- Commander Submarine Force, U.S. Atlantic Fleet, Norfolk, Va.

DEPARTMENT OF THE TREASURY

- Office of the Secretary
- U. S. Customs Service
- Internal Revenue Service
- U. S. Secret Service
- Bureau of Alcohol, Tobacco, and Firearms
- Bureau of Engraving and Printing
- Bureau of Public Debt
- Bureau of Government Financial Operations
- Comptroller of the Currency
- Bureau of the Mint

DEPARTMENT OF TRANSPORTATION

- Office of the Secretary
- Federal Aviation Administration
- United States Coast Guard (Headquarters, Miami, New Orleans)
- Maritime Commission

ENVIRONMENTAL PROTECTION AGENCY

EXECUTIVE OFFICE OF THE PRESIDENT

- Council of Economic Advisors
- National Security Council
- Office of Administration
- Office of Management and Budget
- Office of Science and Technology Policy
- Office of the United States Trade Representative
- Office of the Vice President
- President's Foreign Intelligence Advisory Board
- President's Intelligence Oversight Board

EXPORT IMPORT BANK

FARM CREDIT ADMINISTRATION

FEDERAL COMMUNICATIONS COMMISSION

FEDERAL EMERGENCY MANAGEMENT AGENCY

FEDERAL HOME LOAN BANK BOARD

FEDERAL MARITIME COMMISSION

FEDERAL RESERVE SYSTEM

GENERAL SERVICES ADMINISTRATION

INTERNATIONAL TRADE COMMISSION

INTERSTATE COMMERCE COMMISSION

MARINE MAMMAL COMMISSION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

- Office of Aeronautics and Space Technology
- Office of Space Science and Applications
- Office of Space Flight
- Office of Space Tracking and Data Systems
- Goddard Space Flight Center
- John F. Kennedy Space Center

NATIONAL ARCHIVES AND RECORDS SERVICE

NATIONAL LABOR RELATIONS BOARD

NATIONAL SECURITY AGENCY

NATIONAL SCIENCE FOUNDATION

NATIONAL TRANSPORTATION SAFETY BOARD

NUCLEAR REGULATORY COMMISSION

- Office of International Programs
- Office of the Deputy Executive Director for Operations
  - Division of Security
  - Rules and Records Division
  - Records Services Branch
  - Standardization and Special Projects Branch

OFFICE FOR MICRONESIAN STATUS NEGOTIATIONS

OFFICE OF PERSONNEL MANAGEMENT

OFFICE OF THE SECRETARY OF DEFENSE

- Under Secretary of Defense for Policy
- Assistant Secretary of Defense for International Security Policy
- Assistant Secretary of Defense for International Security Affairs
- Net Assessment
- Defense Guidance Staff
- Emergency Planning
- Assistant Secretary of Defense for Health Affairs
- Assistant Secretary of Defense for Legislative Affairs
- General Counsel
- Under Secretary of Defense for Research and Engineering
- Intelligence Oversight
- Assistant Secretary of Defense, Comptroller
- Assistant Secretary of Defense, Manpower, Installations and Logistics
- Assistant Secretary of Defense for Reserve Affairs
- Assistant Secretary of Defense for Public Affairs
- Inspector General
- Plans, Analysis and Evaluation
- Defense Security Assistance Agency
- Assistant to the Secretary of Defense for Atomic Energy

ORGANIZATION OF THE JOINT CHIEFS OF STAFF

- Office of the Secretary
- Office of the Director, Joint Staff
- Office of the Chairman
- Manpower and Personnel Directorate
- Operations Directorate
- Logistics Directorate
- Plans and Policy Directorate
- Support Services Directorate
- Joint Analysis Directorate
- Command, Control and Communications Systems Directorate
- Joint Planning Staff for Space
- Strategic Plans and Resource Analysis Agency
- Joint Special Operations Agency
- United States Readiness Command, Tampa, Fla.
- United States Central Command, Tampa, Fla.

OVERSEAS PRIVATE INVESTMENT CORPORATION

PEACE CORPS

SMALL BUSINESS ADMINISTRATION

UNITED STATES INFORMATION AGENCY

- Office of Security
    - Physical Security Division
- Office of American Republics Affairs
- Office of North African, Near Eastern, and South Asian Affairs
- Office of Public Liaison
- Office of Administration and Technology
    - Classified Library

UNITED STATES POSTAL SERVICE

- Office of the Chief Postal Inspector
    - Inspection Service

VETERANS ADMINISTRATION

Appendix B

Summary of FY 1983 Program Activity

The FY 1983 Report to the President is the first to examine operations under E.O. 12356. The following data highlight ISOO's findings for FY 83:

Classification Activities

- The number of original classification authorities continued to decline in FY 83. The number of original classifiers has declined from nearly 60,000 in 1972, to 7,010 at the end of FY 83, almost a 90% reduction.
- Agencies made 864,099 original classification decisions, almost 200,000 (18%) fewer than in FY 82.
- By classification level, 2% of original classification decisions were "Top Secret", 32% were "Secret", and 66% were "Confidential".
- Agencies assigned a date or event for automatic declassification to 35% of all information originally classified, as compared to an estimated 10% rate experienced under E.O. 12065.
- Agencies made approximately 17 million derivative classification decisions, a 4% increase over FY 82.
- 5% of all classification decisions were original, 95% were derivative.
- The total of all classification decisions was approximately 18 million, a 3% increase over FY 82.

Declassification Activities

- Agencies received 3,945 new mandatory review requests, 47% fewer than in FY 82.
- Agencies processed 3,610 mandatory review requests, and declassified the information in whole or in part in over 90% of the cases. In processing these requests, agencies reviewed over 29,000 documents comprising nearly 175,000 pages.
- Agencies received 411 new mandatory review appeals.
- Agencies processed 363 mandatory review appeals, declassifying additional information in whole or in part in almost 50% of the cases.
- Agencies systematically reviewed for declassification 12,407,523 pages of classified information, and declassified 7,848,295 (63%). The number of pages reviewed was 36% less than in FY 82. The agencies that now voluntarily perform systematic review accounted for 77% of total number of pages reviewed.

Inspections

- Agencies conducted 22,245 self-inspections, 21% fewer than in FY 82.
- Agencies reported 18,344 infractions, almost 10% fewer than in FY 82.

Annual Report to the President FY 1984

Information Security
Oversight Office

General Services Administration
Information Security Oversight Office
Washington, DC 20405

April 26, 1985

The President
The White House
Washington, DC 20500

Dear Mr. President:

I am pleased to submit the Information Security Oversight Office's (ISOO) 1984 Report to the President.

Established under Executive Order 12065 and continued under Executive Order 12356, effective August 1, 1982, the ISOO oversees the information security system throughout the executive branch. The ISOO is an administrative component of the General Services Administration, but receives its policy direction from the National Security Council.

Last year I was able to report that the system you had established under E.O. 12356 had worked remarkably well during its first full year of operation. This year I can state that this initial success has continued. The agencies of the executive branch are providing better protection for national security information, while also working diligently to control and eliminate unwarranted classification and other shortcomings.

Critical to the success of the system has been the support that you and your senior officials throughout the executive branch have contributed. I urge your continued involvement and assistance.

Respectfully,

Steven Garfinkel

STEVEN GARFINKEL
Director

Contents

Page

Letter to the President.................................. i
Agency Acronyms or Abbreviations.......................... iv
Summary of FY 1984 Program Activity....................... v
The Information Security Program FY 1984.................. 1

Program Reviews and Inspections.................... 2
Statistical Reporting.............................. 2
Original Classification Authorities................ 3
Original Classification............................ 5
Derivative Classification.......................... 9
Total Classification Activity...................... 10
Mandatory Review for Declassification.............. 11
Systematic Declassification Review................. 15
Agency Self-Inspections............................ 13

Narrative Look at FY 1984................................. 20
Appendix: ISOO Inspections: FY 1983 and FY 1984.......... 27

Exhibits

1. Reduction in Original Classifiers................. 4
2. Number of Original Classifiers.................... 4
3. Comparison of Original Classification Activity.... 5
4. Original Classification Decisions................. 6
5. FY 1984 Original Classification Decisions by Agency.. 7
6. Original Classification Decisions Scheduled for Automatic Declassification...................... 8
7. Comparison of Derivative Classification Activity.. 9
8. FY 1984 Derivative Classification Actions by Agency.. 10
9. Comparison of Combined Classification Activity.... 10
10. Original vs. Derivative Classification............ 11
11. Mandatory Review Requests Received................ 12
12. Mandatory Review Actions.......................... 13
13. FY 1984 Mandatory Review Actions by Agency........ 14
14. Mandatory Review Appeals Received................. 15
15. Pages Reviewed for Declassification............... 16
16. Percentage of Reviewed Pages Declassified......... 17
17. FY 1984 Systematic Review Actions by Agency....... 17
18. Agency Self-Inspections........................... 18
19. Infractions....................................... 19

Agency Acronyms or Abbreviations Used in this Report

ACDA : Arms Control and Disarmament Agency
AID : Agency for International Development
CIA : Central Intelligence Agency
DoD : Department of Defense
DoE : Department of Energy
DoT : Department of Transportation
FBI : Federal Bureau of Investigation
FEMA : Federal Emergency Management Agency
GSA : General Services Administration
ISOO : Information Security Oversight Office
JUSTICE : Department of Justice
NARA : National Archives and Records Administration
NARS : National Archives and Records Service
NASA : National Aeronautics and Space Administration
NRC : Nuclear Regulatory Commission
NSC : National Security Council
OSTP : Office of Science and Technology Policy
OVP : Office of the Vice President
PIOB : President's Intelligence Oversight Board
STATE : Department of State
TREASURY : Department of the Treasury
USIA : United States Information Agency
USTR : Office of the United States Trade Representative

Summary of FY 1984 Program Activity

The FY 1984 Report to the President is the second to examine the information security program under E.O. 12356. The following data highlight ISOO's findings:

Classification Activities

- The number of original classification authorities declined 2% in FY 84, to 6,900, the first time the figure has fallen below 7,000.
- Original classification decisions increased slightly in FY 84, to 881,943; this was still considerably less than the 1,055,152 original decisions made in FY 82, under E.O. 12065.
- By classification level, 2% of original classification decisions were "Top Secret", 30% were "Secret", and 68% were "Confidential".
- Under E.O. 12356, originally classified information has been marked for automatic declassification 33.5% of the time, as compared to an estimated 10% of the time under E.O. 12065.
- Derivative classification decisions rose 9% over FY 83, to 18,725,793.
- 4% of all classification actions were original, 96% were derivative.
- The total of all classification actions, 19,607,736, represented a 9% increase over FY 83.

Declassification Activities

- Agencies received 4,650 new mandatory review requests, the second highest total since the program was established in FY 72.
- Agencies processed 4,401 requests, and declassified the information in whole or in part in 91% of the cases, releasing in whole or in part 104,821 documents totaling 325,530 pages.
- Agencies received 408 new mandatory review appeals.
- Agencies took action on 424 appeals, declassifying additional information in whole or in part in 82% of the cases.
- Under the systematic review program, agencies declassified 10.9 million pages of permanently valuable records, 3 million more than in the previous year.

Inspections

- Agencies undertook 27,831 self-inspections, a 25% increase over FY 83.
- Agencies reported 19,157 infractions, a 4.4% increase over FY 83.

Information Security Oversight Office
The Information Security Program
FY 1984

Under Executive Order 12356, the Information Security Oversight Office (ISOO) is responsible for monitoring the information security programs of those executive branch activities that generate or handle national security information. Originally established by Executive Order 12065, ISOO continues to be the primary oversight organization in the system prescribed by President Reagan's Order of April 2, 1982. In this role, ISOO oversees the information security programs of approximately 65 departments, independent agencies and offices of the executive branch. E.O. 12356 also requires the Director of ISOO to report annually to the President about the ongoing implementation of the Order's provisions. This Report highlights Government-wide performance during FY 1984, the system's second year.

ISOO is located administratively in the General Services Administration but receives its policy direction from the National Security Council. The Administrator of General Services appoints the ISOO Director upon approval of the President. The ISOO Director appoints the staff, which numbers between 13-15 persons. For FY 1984, ISOO's budget was $649,000.

ISOO fulfills its assigned responsibilities under E.O. 12356 in a variety of ways. First, it develops and issues implementing directives and instructions regarding the Order. During FY 1984, this also included the issuance of rules regarding agency use of a Classified Information Nondisclosure Agreement (Standard Form 189) to be executed by each employee as a condition of access to classified information. Second, ISOO conducts on-site inspections or program reviews of monitored agencies on a regular basis. Third, it gathers, analyzes and reports statistical data on agencies' programs. Fourth, it evaluates, develops or disseminates security education materials and programs. Fifth, ISOO receives and takes action on suggestions, complaints, disputes and appeals from persons inside or outside the Government on any aspect of the administration of the Order. In this area, ISOO serves as the final appellate authority for the mandatory declassification review of presidential materials. Sixth, it conducts special studies on identified or potential problem areas and on programs to improve the system. Seventh, ISOO maintains continuous liaison with monitored agencies on all matters relating to the information security system. This Report is based upon program reviews and inspections conducted by the ISOO staff and the compilation and analysis of statistical data regarding each agency's program activity.

Program Reviews and Inspections

ISOO's program analysts serve as liaison to specific agencies to facilitate coordination and to provide for continuity of oversight operations. The analysts must stay abreast of relevant activities within each agency's information security program; coordinate with assigned agency counterparts on a continuing basis; and conduct formal inspections of the agency's program in accordance with a planned annual inspection schedule, which includes visits to selected field activities as well as offices in the Washington metropolitan area. The appendix to this Report lists those activities that ISOO inspected during FY 1983 and FY 1984.

These on-site inspections encompass all aspects of the information security program, including classification, declassification, safeguarding, security education, and administration. The inspections always include detailed interviews with agency security personnel, classifiers, and handlers of national security information. To the extent possible, ISOO analysts review a sampling of classified information in the agency's inventory to examine the propriety of classification, the existence of necessary security markings and declassification instructions, and compliance with safeguarding procedures. ISOO analysts also monitor security training programs to determine if they adequately inform personnel about classifying, declassifying, marking and safeguarding national security information. When weaknesses in an agency's program are identified, ISOO analysts recommend corrections, either on-the-spot or as part of a formal inspection report. Critical reports require immediate remedial attention by the agency prior to a follow-up inspection by ISOO. These inspections are a necessary means of identifying and resolving problem areas. They provide specific indicators of agency compliance or noncompliance with E.O. 12356 that are not apparent simply from the analysis of statistical data.

Statistical Reporting

To gather relevant statistical data regarding each agency's information security program, ISOO developed the Standard Form 311, which requires each agency to report annually the following information:

1. The number of original classification authorities;
2. the number of declassification authorities;
3. the number of original classification decisions, including the classification level of those decisions and the duration of classification;

4. the number of derivative classification decisions by classification level;

5. the number of requests received for mandatory review for declassification and agency actions in response to these requests in terms of cases, documents, and pages;

6. the number of pages of national security information reviewed during the year under systematic declassification procedures and the number declassified;

7. the number of formal self-inspections conducted by the agency; and

8. the number of security infractions detected by the agency within its own program.

The statistics reflected in this Report cover the period October 1, 1983 through September 30, 1984.

Further Reductions of Original Classification Authorities

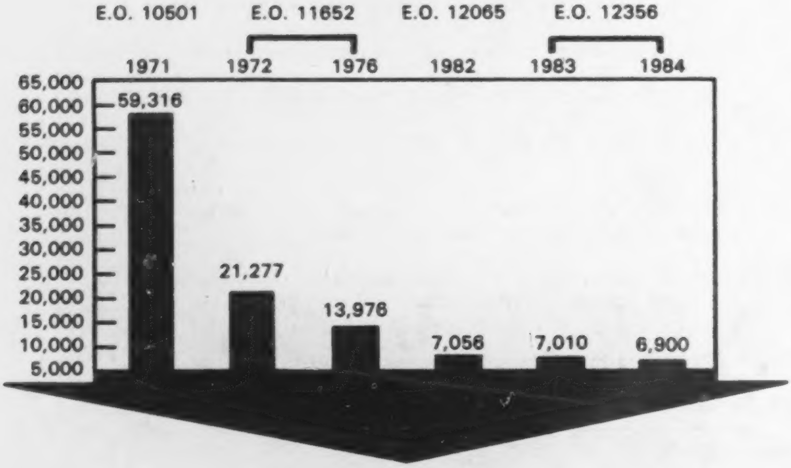
(Exhibits 1 and 2)

Original classification authorities are those individuals specifically authorized in the first instance to classify information in the interest of national security. These classifiers are designated in writing, either by the President or by other officials, primarily agency heads, named by the President. Limiting the number of original classifiers to the minimum necessary for efficient management is one way to control the volume of overall classification activity. ISOO prods agencies to conduct regular surveys to ensure that the number of original authorities is in line with operational requirements.

In 1972, there were 59,316 individuals in the executive branch authorized to classify originally. This number has decreased dramatically since that time. In FY 1984, there were only 6,900 original classification authorities. This figure represents a decrease of 2% from the 7,010 original classifiers reported in FY 1983. The overall reduction results from a decline of 180 (14%) in the number of "Confidential" classifiers. This figure more than offsets the rise in the number of "Top Secret" classifiers by 35 (2%), and "Secret" by 35 (1%).

Exhibit 1

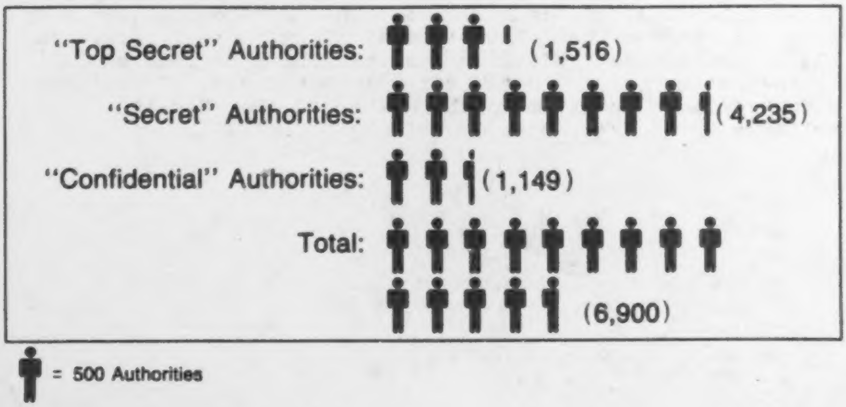
The Reduction in Original Classifiers 1971 - 1984



Several agencies deserve special credit for significantly reducing the number of original classifiers in FY 1984. They include ACDA (-31%); DoD (-9%); NRC (-8%); Treasury (-30%); and OVP (-33%). Of particular note is ACDA, which has reduced its number of original classifiers from 88 in FY 1982, to 33 in FY 1984. In FY 1985, ISOO will focus particular attention on those activities which increased their number of original classifiers in the past year.

Exhibit 2

Number of Original Classifiers



Original Classification Remains at Reduced Level

(Exhibits 3 through 6)

An original classification decision is an initial determination by an authorized official that information requires protection from unauthorized disclosure in the interest of national security. The determination is accompanied by the placement of required classification markings on the medium that contains the information. The number of original classification decisions is probably the most important statistic reported by ISOO each year because of its wide ranging impact on all aspects of the information security program.

During FY 1984, the number of original classification decisions totaled 881,943. This represents an increase of 17,844 from the number reported in FY 1983. "Top Secret" actions increased by 3,824 (24%), "Confidential" rose by 29,946 (5%), while the number of "Secret" actions dropped by 15,926 (6%). Despite the increases reported for FY 1984, the number of original classification actions were only 2% higher than the prior year's unprecedented low figure. The total remains 16% lower than the 1,055,152 actions reported for FY 1982, the last year under the previous Executive Order.

Exhibit 3

Comparison of Original Classification Activity

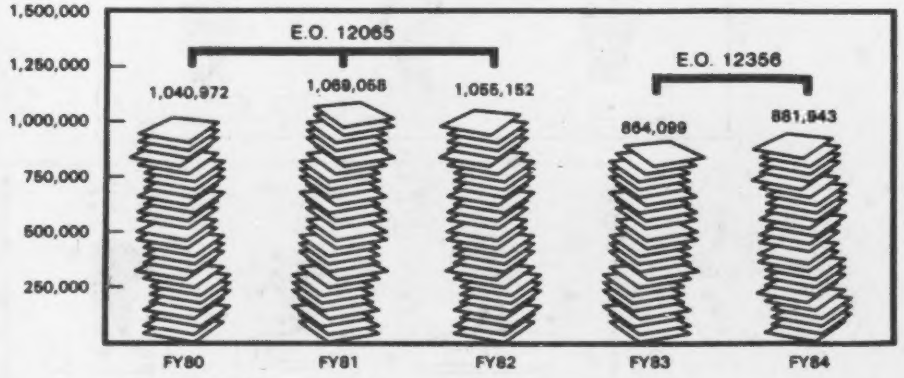
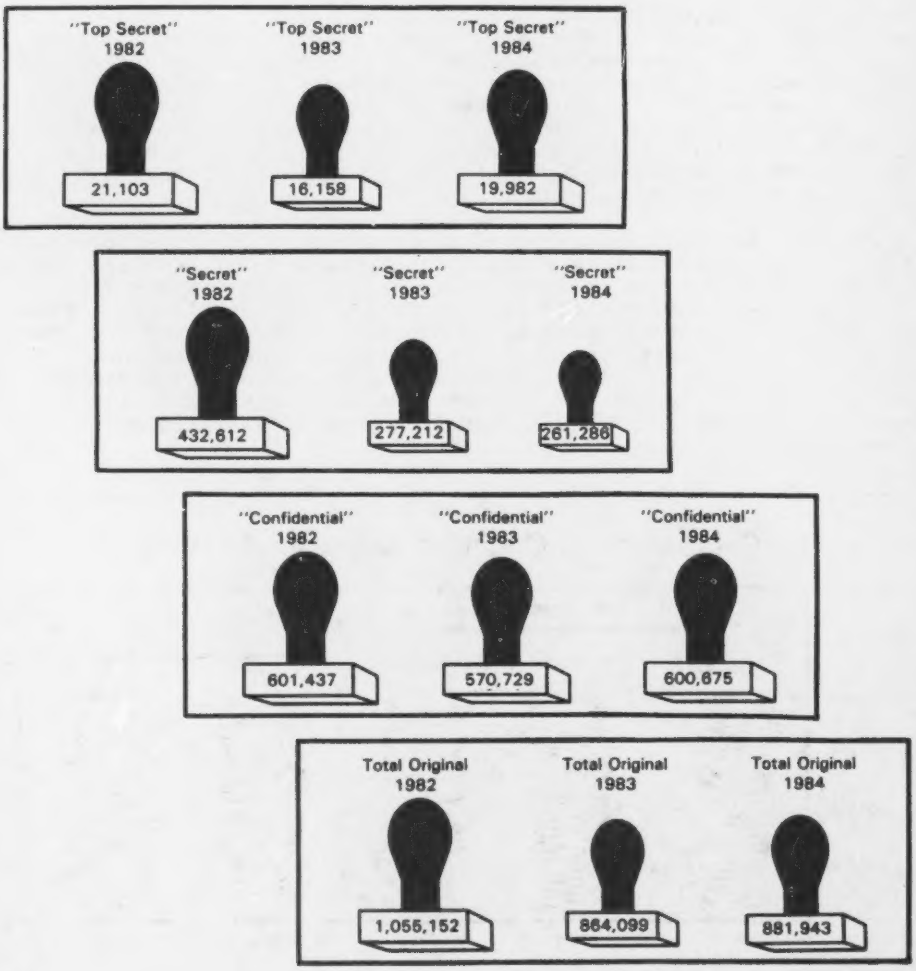


Exhibit 4

Original Classification Decisions



In FY 1984, "Top Secret" decisions comprised 2% of original classification actions, "Secret" accounted for 30%, and "Confidential" the remaining 68%. These figures closely approximate those reported for FY 1983. "Confidential" determinations still constitute a significant majority of original classification actions made in the executive branch. This has important implications in terms of the costs borne by the Government to protect national security information. More stringent requirements in terms of storage and transmission apply to "Secret" and especially "Top Secret" information. Therefore, classifying at the "Confidential" level rather than "Secret" or "Top Secret" saves the Government considerable resources. More importantly, holding the line on classification and classification levels helps preserve the integrity of the classification system itself.

Four agencies continue to classify originally more than 99% of the actions within the executive branch. Of these, CIA registered a 16% increase (following a 44% decrease in FY 1983), DoD a rise of 11%, and State an increase of 8% during FY 1984. These increases were nearly offset by a dramatic decrease of 51% at Justice. In preparation for this Report, ISOO worked with the agencies primarily responsible for the rise in original classification decisions to ascertain the reasons for the increases. ISOO is satisfied that the increases in original classification actions are reasonably accounted for by a number of factors. These included several specific world events that gave rise to large numbers of classified communications as well as new defense and intelligence initiatives.

Exhibit 5

FY 1984 Original Classification Decisions by Agency

Agency	Original Decisions	% Assigned Date or Event for Declassification	% OADR (Must Be Reviewed before Declassification)	% "TS"	% "S"	% "C"
DoD	345,919	71%	29%	1%	18%	81%
CIA	266,188	5%	95%	5%	42%	53%
State	196,052	12%	88%	0%	22%	78%
Justice	64,942	0%	100%	3%	63%	34%
Treasury	2,028	16%	84%	0%	7%	93%
FEMA	1,945	5%	95%	30%	44%	26%
DoE	1,506	15%	85%	0%	60%	40%
AID	1,099	68%	32%	0%	1%	99%
All Others	2,264	34%	66%	5%	35%	60%

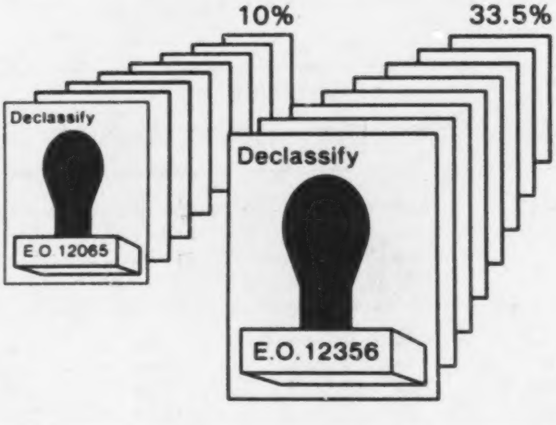
During FY 1984, 32% of the actions specified automatic declassification upon the passage of a particular date or event. Although this figure is slightly less than for FY 1983, the 33.5% average under E.O. 12356 still represents a substantial improvement over the predecessor system, which ISOO estimates required agency review prior to declassification in 90% of original classification actions.

Automatic scheduling for declassification should facilitate the declassification process as a whole and increase the amount of material made available to scholars and the public.

DoD continues to merit special recognition with an automatic declassification rate of 71%, the same proportion as reported in FY 1983. Other agencies had significantly lower ratios. ISOO will continue to encourage these activities to use a specific date or event as the declassification instruction whenever possible, and will examine documents to determine whether such instructions could reasonably substitute for the indefinite designation "Originating Agency's Determination Required" ("OADR").

Exhibit 6

Original Classification Decisions Scheduled for Automatic Declassification



Derivative Classification Actions Increase

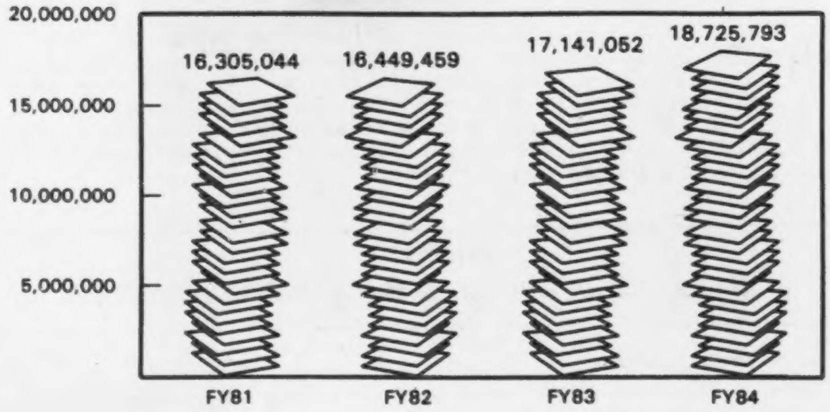
(Exhibits 7 and 8)

Derivative classification is the act of incorporating, paraphrasing, restating or generating in new form classified source information. Information may be derivatively classified in two ways: (a) through the use of a source document, usually correspondence or publications generated by an original classification authority; or (b) through the use of a classification guide. Only executive branch or Government contractor employees with the appropriate security clearance who are required by their work to restate classified source information may classify derivatively.

During FY 1984, executive branch agencies made 18,725,793 derivative classification decisions, a 9% increase over FY 1983. Of the total derivative classification actions taken during the reporting period, 459,385 (2%) were classified at the "Top Secret" level, 5,525,987 (30%) at the "Secret" level, and 12,740,729 (68%) at the "Confidential" level. "Top Secret" derivative decisions decreased from 3% to 2% of the total number of decisions. There were 63,143 fewer "Top Secret" derivative decisions in FY 1984 than in FY 1983, a decrease of 12%.

Exhibit 7

Comparison of Derivative Classification Activity



Of the three agencies responsible for nearly all of the derivative classification actions, DoD and Justice reported increases of 1,602,689 and 99,213 actions respectively. The CIA experienced a decline of 128,827 actions. Other agencies reporting substantial percentage reductions in the number of derivative classification decisions in FY 1984 as compared to FY 1983 included the PIOB (-92%), NSC (-34%), OSTP (-41%), USTR (-62%), and Treasury (-44%).

Exhibit 8
FY 1984 Derivative Classification Actions by Agency

Agency	Total Derivative Actions	% "TS"	% "S"	% "C"
DoD	16,264,038	2%	21%	77%
CIA	2,289,872	3%	83%	14%
Justice	124,927	1%	99%	0%
DoE	18,262	0%	17%	83%
NASA	11,265	0%	99%	1%
FEMA	4,453	8%	65%	27%
Treasury	1,527	2%	62%	36%
All Others	11,449	27%	29%	44%

Combined Classification Activity Increases

(Exhibits 9 and 10)

During FY 1984, the combined number of original and derivative classification decisions made by executive branch agencies was 19,607,736. This was approximately 1,600,000 (9%) more than in FY 1983, an increase that is larger than the corresponding increases reported during the past several years. The overriding reason is the 9% rise in derivative actions; original decisions had almost no bearing on the increase.

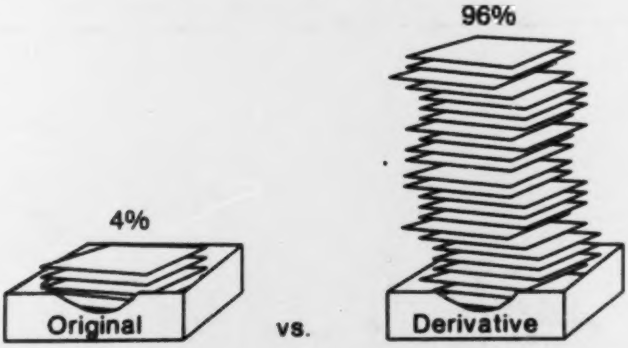
Exhibit 9
Comparison of Combined Classification Activity

FY	Total Actions	%"TS"	%"S"	%"C"
1981	17,374,102	5%	29%	66%
1982	17,504,611	3%	31%	66%
1983	18,005,151	3%	30%	67%
1984	19,607,736	2%	30%	68%

For FY 1984, the data show 2% of all classification decisions were classified at the "Top Secret" level, 30% at the "Secret" level, and 68% at the "Confidential" level. This ratio reflects a 1% decrease in "Top Secret" decisions, and a 1% increase in "Confidential" decisions. As in previous years, DoD (84.7%) and CIA (13%) accounted for almost 98% of the classification activity in the executive branch. During FY 1984, the ratio of original to derivative classification actions changed for the second year in a row. Prior to FY 1983, original classification comprised 6% of all classifications, and derivative 94%. By FY 1984, the ratio was 4% original, 96% derivative. The reason for this change and its impact are examined in the narrative that follows this section of the Report.

Exhibit 10

Original vs. Derivative Classification



Mandatory Review Yields Impressive Results

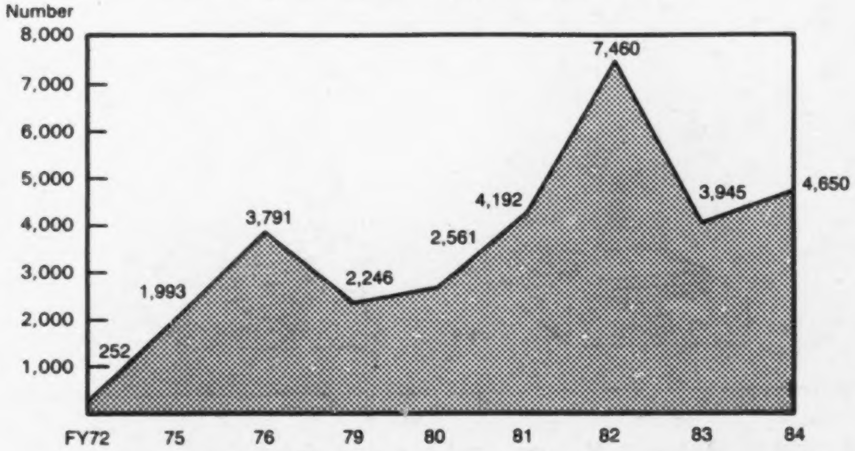
(Exhibits 11 through 14)

Under E.O. 12356, the mandatory review process allows agencies or citizens to require an agency to review particular national security information for purposes of seeking its declassification. Such requests must be in writing and must describe the information with enough detail to permit the agency to retrieve it with a reasonable amount of effort. Mandatory review is a process popular with researchers as a less combative alternative to Freedom of Information Act requests.

After leveling off in FY 1983, the number of mandatory review requests increased again in FY 1984 to 4,650. This is the second highest number of requests received since the program was established in FY 1972. Added to the 1,334 cases carried forward from FY 1983, agencies had a mandatory review caseload of 5,984 during FY 1984. Of these, the agencies processed 74% of the total, a 28% increase over the proportion processed in FY 1983. In last year's report, ISOO indicated that one of its immediate goals would be to seek to reduce the inventory of pending cases. While progress toward this goal was offset by the 18% increase in new cases received, agencies exhibited excellent initiative by acting on 22% more cases, 262% more documents, and 98% more pages than in FY 1983.

Exhibit 11

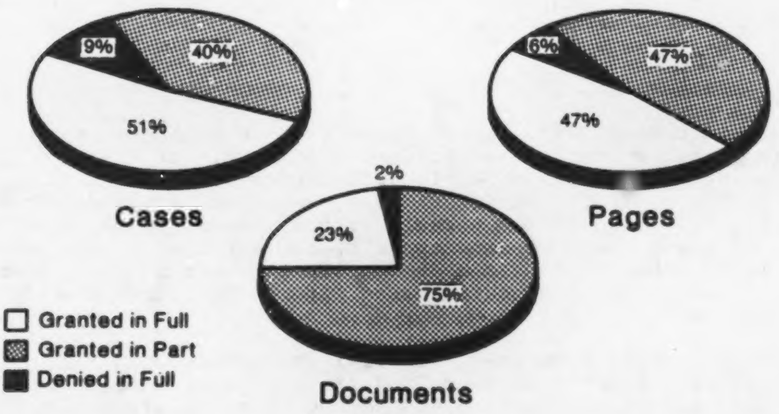
Mandatory Review Requests Received



ISOO collects data on agency actions in response to mandatory review requests in terms of cases, documents and pages. Of the 4,401 cases acted on in FY 1984, 2,259 (51%) were granted in full, 1,759 (40%) were granted in part, and 383 (9%) were denied in full. Although the percentage of cases granted in full decreased marginally in FY 1984, the percentage of cases denied in full remained below 10% for the second consecutive year.

Exhibit 12

Mandatory Review Actions



The 4,401 cases comprised 106,683 documents or 344,999 pages of national security information, an increase of 77,219 documents and 170,986 pages over the figures for FY 1983. Of the 106,683 documents, 24,904 (23%) were declassified in full, 79,917 (75%) were declassified in part, and 1,862 (2%) remained fully classified. Although the percentage of documents fully declassified dropped markedly, the percentage of documents which remained fully classified also decreased. A clearer indication that the mandatory review program resulted in a greater amount of information being declassified is reflected in the number of pages released in full or in part during the year. Of the 344,999 pages reviewed in FY 1984, 325,530 were either declassified in full or in part, over twice as many as the 154,238 pages reported for FY 1983.

Exhibit 13

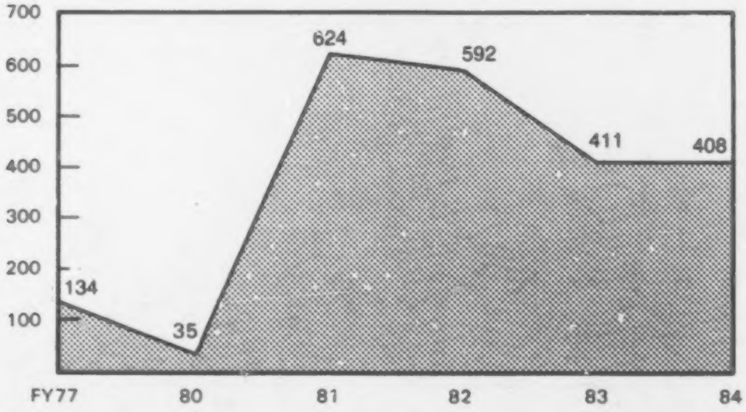
FY 1984 Mandatory Review Actions by Agency

Agency	Total Cases Acted On	% Granted In Full	% Granted In Part	% Denied In Full
DoD	1,732	52%	42%	6%
State	684	47%	45%	8%
NSC	645	49%	44%	7%
GSA (Including NARS)	422	40%	41%	19%
Justice	339	78%	19%	3%
CIA	274	33%	44%	23%
All Others	305	63%	25%	12%

The Executive Order also gives requesters the right to appeal mandatory review denials to designated officials of the denying agencies, or, with regard to classified presidential materials, to the Director of ISOO. During FY 1984, agencies received 408 new appeals in addition to 802 appeals carried over from the previous year. Of these 1,210 pending appeals, the agencies completed 424 (35%) in FY 1984. This was a 4% improvement over FY 1983, but ISOO will continue to urge increased efforts to reduce the remaining backlog.

Of the 424 appeals processed, 92 (22%) were granted in full, 256 (60%) were granted in part, and 76 (18%) were denied in full. These 424 appeals comprised 5,929 documents or 26,470 pages. Of the 5,929 documents reviewed on appeal, 1,997 (34%) were declassified in full, 3,726 (63%) were declassified in part, and 206 (3%) remained fully classified. Of the 26,470 pages reviewed, 6,729 (26%) were declassified in full, 18,062 (68%) were declassified in part, and 1,679 (6%) remained fully classified. For FY 1984, the numbers of documents and pages declassified and released in full or in part were substantially higher than in FY 1983. This suggests that the agencies are making every effort to release as much information as possible consistent with national security concerns.

Exhibit 14
Mandatory Review Appeals Received



Systematic Review May Be On The Mend

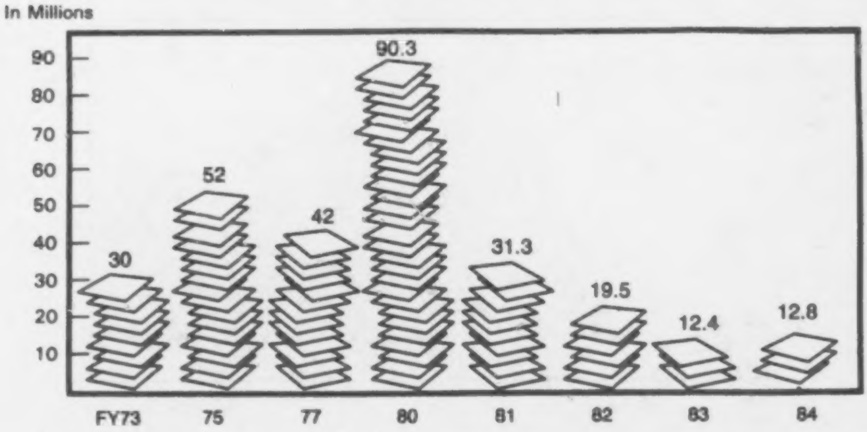
(Exhibits 15 through 17)

"Systematic review for declassification" is the program, first introduced in 1972, in which classified, permanently valuable (archival) records are reviewed for purposes of declassification after the records reach a specific age. Under E.O. 12356, NARS (now NARA) is required to conduct a systematic review of its classified holdings as they become 30 years old, except for certain intelligence or cryptologic file series which are to be reviewed as they become 50 years old. While other agencies are not required to conduct a systematic review program, they are encouraged to do so if resources are available.

In recent years, the product of the systematic review program has declined as a result of two factors. First, the records that are now being reviewed are not generally susceptible to the bulk declassification methods that were frequently adequate in declassifying World War II era records. Second, the resources available for systematic review have continued to dwindle. From FY 1980 to FY 1983, the number of pages reviewed under the systematic declassification program decreased from 90.3 million to 12.4 million.

Exhibit 15

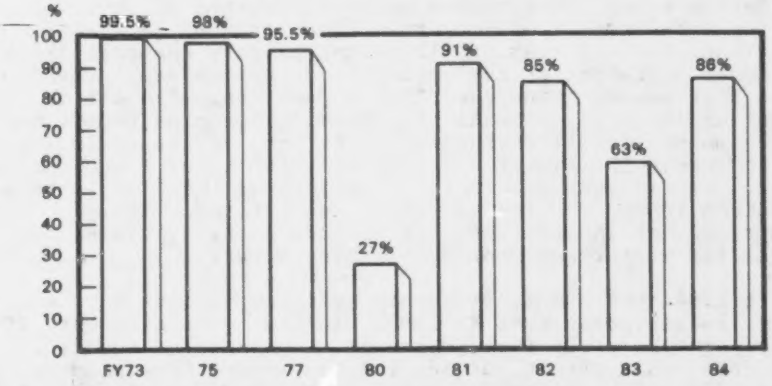
Pages Reviewed for Declassification



Increased attention to the systematic review program in the past year may signal a reversal of that trend. For FY 1984, agencies reported that they had reviewed nearly 12.8 million pages, an increase of 366,000 pages over FY 1983. Of even greater importance is the substantial increase in the percentage of reviewed pages that were declassified under the program in FY 1984. In FY 1983, only 63% of the pages reviewed were declassified; that figure jumped to approximately 86% for the period covered by this Report. In other words, of the 12.8 million pages reviewed in FY 1984, 10.9 million were declassified. This represents an increase of more than 3 million pages in the amount of historically valuable Government records made available to the public as a result of the program compared to the prior year. These improved figures are primarily the work of DoD, at which the percentage of pages declassified rose from 54% in FY 1983, to 85% in FY 1984. DoD accounts for over 75% of all the pages reviewed under the systematic declassification program. NARA, which is required under E.O. 12356 to conduct a systematic review program, and which accounts for the second highest volume, increased by 1% the number of pages examined, and declassified 91%. It is hoped that the resources made available for the NARA program will be greater in the next fiscal year. A task force established by the Archivist in FY 1984, on which the ISOO Director served, recommended a substantial increase in the size of the NARA staff devoted to the program, and there has been some progress in this direction.

Exhibit 16

Percentage of Reviewed Pages Declassified



Although agencies other than NARA are not required to conduct systematic review programs under E.O. 12356, several continue to do so. In addition to DoD, State and USIA have active programs, although the number of pages reviewed by the latter two agencies dropped 47% and 74%, respectively. In the case of USIA, the decrease resulted from the fact that its resources had to be devoted to a significant increase in its mandatory review workload. On the other hand, DoE's systematic review effort increased substantially in FY 1984, and the proportion of pages declassified by DoE was nearly 100%.

Exhibit 17

FY 1984 Systematic Review Actions by Agency

Agency	Pages Reviewed	Pages Declassified	% Declassified
DoD	9,628,592	8,186,052	85%
GSA/NARS	2,889,600	2,641,954	91%
State	56,517	51,330	91%
USIA	40,000	39,950	99%
DoT	25,000	2,548	10%
All Others	133,881	8,944	7%

Agency Self-Inspections Increase

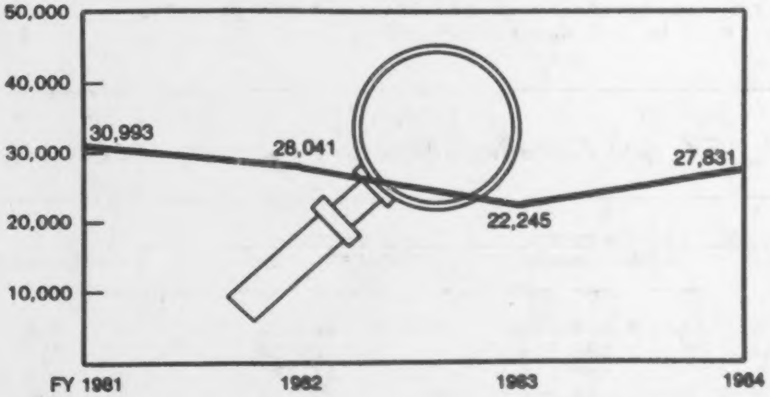
(Exhibits 18 and 19)

While the Executive Order authorizes the Director of ISOO to conduct on-site inspections of those agencies that generate and handle classified information, it places primary responsibility for internal oversight on the agency heads themselves. The Order requires that agency heads establish and maintain "an active oversight and security education program." Agencies report to ISOO the number of self-inspections that they undertake each year. They also report the number and type of infractions found during the year. Infractions are minor violations of the Order, the implementing ISOO Directive or agency regulations. These statistics do not include the more serious security violations that agencies must report to ISOO as they occur.

During FY 1984, the number of agency self-inspections totaled 27,831, a 25% increase over FY 1983. In last year's report, ISOO expressed concern about the decline in the number of agency inspections. As a result, during its own inspections program, ISOO analysts have repeatedly stressed the need for agencies to develop internal monitorship programs to ensure effective implementation of the Order. One of the consequences of the increased number of self-inspections undertaken by the agencies was a corresponding rise in the number of infractions reported.

Exhibit 18

Agency Self-Inspections



The total number of infractions reported for FY 1984 was 19,157, an increase of 4.4% over FY 1983. Although ISOO applauds the 25% rise in self-inspections conducted by the agencies, they continue to detect less than one infraction per inspection, which is far below the average that ISOO analysts find during their on-site surveys.

Exhibit 19
Infractions

Infraction	Total FY 81	Total FY 82	Total FY 83	Total FY 84	% Change 83-84
Unauthorized Access	476	475	620	483	-22%
Mismarking	8,797	11,499	10,849	7,503	-31%
Unauthorized Transmission	924	1,197	1,294	1,773	+37%
Improper Storage	3,341	4,222	3,844	7,363	+92%
Unauthorized Reproduction	135	207	249	190	-24%
Overclassification	N/R	290	220	302	+24%
Underclassification	N/R	365	317	351	+11%
Classification w/o Authority	N/R	392	238	597	+150%
Improper Destruction	N/R	665	581	475	-18%

N/R = Statistics not reported for FY 1981

A Narrative Look At FY 1984

The President's issuance of Executive Order 12356 prompted unprecedented scrutiny and discussion of the Government-wide information security program. Never before had the classification, declassification, and safeguarding of national security information generated so much attention and comment. Then, with the issuance of the Information Security Oversight Office (ISOO) FY 1983 Report to the President, the commotion abruptly subsided. For many, unfortunately, good news was no news.

ISOO's analysis of FY 1984, the second full year of E.O. 12356's operation, brings more good news. It is now very clear that the outstanding accomplishments of the prior year were no fluke. While a number of hurdles remain, ISOO concludes once again that the President's stated goal of achieving better protection for national security information while working to prevent unwarranted classification is clearly being met.

FY 1984 Program Strengths: General

(a) Following quite naturally upon the smooth transition from E.O. 12065 to E.O. 12356 has been the continued stability of the revised system. Last year ISOO noted two contributing factors to the smooth transition: First, the two systems paralleled one another in most day-to-day situations; and second, the concerted effort of senior program officials throughout the executive branch to achieve a smooth transition. For FY 1984, ISOO cites a third factor as contributing significantly to the continued stability of the system. This is the increased administrative flexibility deliberately built into E.O. 12356.

As noted by ISOO in its FY 1982 Report to the President, one of the predecessor system's glaring shortfalls was its inflexibility in a number of administrative situations. While designed to prevent excessive classification, in practice several of these provisions simply produced excessive red tape. E.O. 12356 modified these provisions to allow controlled flexibility within the system.

From all indications the result is a system that is stable but not static. Within the executive branch concerned officials and employees express widespread satisfaction with the revised system. Outside the executive branch, in particular among those institutions most frequently critical of the information security system, there is quiet, except for an occasional outburst over initiatives to impede unauthorized disclosures of classified information. Perhaps more than anything else this very silence bespeaks the current stability of the information security system.

(b) The absence of serious abuse is critical to the credibility of a system that exists to control access to national security information. In ISOO's view, once again in FY 1984, no serious abuse of the system surfaced. The oversight and responsiveness of senior program officials contributed significantly to its absence.

Of particular concern to ISOO is the potential for abuse of that provision of E.O. 12356 that permits, under very limited circumstances, the reclassification of information that has previously been declassified and disclosed under appropriate authority. Once again in FY 1984, reclassification actions very seldom arose. When they did, ISOO examined their legitimacy in detail. In each instance, ISOO was either satisfied that the reclassification action was necessary and proper or the agency involved withdrew its plans for reclassification.

(c) In its last Report to the President ISOO faulted the lack of familiarity with E.O. 12356 by too many persons who work with classified information. As a result, during FY 1984, ISOO again concentrated much of its oversight on agency security education programs. While there is still significant room for improvement in some agencies, most have instituted training programs that have increased employees' knowledge about the information security system and their responsibilities under it. A greater percentage of persons interviewed by ISOO analysts during its FY 1984 inspections displayed a good working knowledge of information security than had been the case in prior years. With the continuation and augmentation of security education efforts, ISOO anticipates even more improvement in this area.

FY 1984 Program Strengths: Statistical

(a) As ISOO has repeatedly maintained, the most important quantitative measurement of the information security system is the annual tally of original classification decisions. More precisely than any other reported statistic, these decisions represent the number of "new secrets" created during the year. In actual practice, of course, the number of "new secrets" is far lower than the total number of original classification decisions. There is large scale subject matter duplication, and many classification decisions that some agencies count as original are actually derivative.

In FY 1983, the executive branch witnessed a dramatic 18% drop in the number of original classification decisions. FY 1984's minimal 2% increase reveals that this was not a one-shot fluke. Original classification remained well below the levels experienced under E.O. 12065, despite a year that featured a number of world events that generated large numbers of classified communications. In ISOO's view, the major reason for the decrease in original classification relates to the greater use of classification guides, especially in agencies that did not use guides until recently. The discussion below, concerning the rise in derivative classification, examines this phenomenon in greater detail.

(b) The agencies, especially the many components of the Defense establishment, continue to do an excellent job of designating a significant portion of their classified information for automatic declassification upon a specific date or event. The percentage of information so marked under E.O. 12356 remains more than three times greater than under the prior system. Ultimately, that much more information will be available to public access without involving a costly, time-consuming review procedure.

(c) In the wake of a new information security system, which required agency heads to redesignate their original classifiers, FY 1983's reduction of 46 classifiers was a pleasant surprise. The agencies demonstrated responsible restraint at a time when some excess would have been understandable, given the fact that the number of original classifiers had shrunk by more than 50,000 over the prior 12 years.

In FY 1984, the agencies did even better, shaving another 110 classifiers off the rolls. There is some temptation to accept this first dip below the 7,000 range as an achieved goal. Only the knowledge that there are still a number of unnecessary original classification authorities prevents this complacency.

(d) In FY 1982, the number of mandatory review requests took a sudden upswing. Critics explained that researchers had turned to the mandatory review process because the dwindling product of systematic review no longer met their needs. In FY 1983, the number of mandatory review requests leveled off. These same critics explained that researchers had discovered that the mandatory review process wasn't worth the effort. ISOO is hard-pressed to anticipate the "Catch-22" explanation for FY 1984.

In fact, the mandatory review process has been, and continues to be, an outstanding success. Year in and year out, agency reviewers declassify a large percentage of the information sought by researchers. In FY 1984, the mandatory review workload, when expressed by the number of documents and pages examined, increased to what was probably its highest level. (ISOO did not collect data in terms of documents and pages until FY 1983.) As a result, researchers received a higher return than ever before. The agencies, which rarely receive anything for their efforts but more criticism, deserve a great deal of credit.

FY 1984 Program Weaknesses: General

(a) Section 4.1 of Executive Order 12356 expresses the link between the information security and personnel security systems:

> A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

These requirements are routinely paraphrased as "a clearance plus a 'need-to-know.'" In ISOO's view both of these requirements deserve far greater attention.

With respect to the clearance process, commentators for many years have been calling for reform, but the agencies have never been able to agree among themselves what changes are necessary or advisable. In National Security Decision Directive 84, the President instituted a high-level, interagency effort to resolve these problems, and that process is continuing. Whatever the system, however, ISOO believes that far too many individuals receive clearances for access to national security information. Its inspections and its experience with agency implementation of the Classified Information Nondisclosure Agreement constantly reinforce this fact to ISOO. All too often, agencies grant clearances by habit, or as a badge of prestige, rather than as a requisite of job responsibilities. Far greater efforts are needed to limit national security clearances to persons whose work necessitates access to national security information.

Perhaps more damaging is the widespread indifference to the "need-to-know" principle. All too often holders of classified information distribute it to others based solely on their clearances, making little or no effort to ascertain the reasons access is required for the performance of job responsibilities. With the proliferation of clearances, strict adherence to "need-to-know" becomes even more critical.

In ISOO's view, the obvious security threat is not the only unfortunate consequence of relaxed enforcement of personnel security requirements. Another is the increasing usage by agencies of special access programs to help protect classified information. Under E.O. 12356 and its predecessor systems, certain agency heads may create special access programs "to control access, distribution, and protection of particularly sensitive information . . .." These programs are very costly. ISOO believes that many current special access programs would not have been created if agencies had greater confidence in the enforcement of clearance and "need-to-know" principles.

(b) Similar security problems flow from the broad distribution of classified information among and within agencies and offices. Too often, classified information is distributed to others by rote rather than reason. Increasingly, the use of automated systems exacerbates this problem. Programmers frequently design these systems to facilitate the widespread distribution of information rather than its protection. As a result, offices routinely receive the classified product of other offices whether or not they have any need for the information.

A disturbing side effect of the broad distribution of classified information involves its impact on the unauthorized disclosure of national security information. First, widespread availability heightens the opportunity for negligent or deliberate unauthorized disclosure; subsequently, when unauthorized disclosures occur, many investigations of them fail because of the size of the universe of possible leakers.

(c) Even with greatly reduced levels of original classification, overclassification remains a problem and, indeed, a threat to the credibility of the system. From ISOO's broad exposure to national security information, the amount that is classified unnecessarily is far less than critics of the system proclaim. Nevertheless, the "bad apple" syndrome haunts the classification process. Reduced numbers do not permit the relaxation of oversight.

In FY 1984, ISOO became increasingly concerned about the phenomenon of "prestige" classification. This may occur when the director of a program with national security implications decides that the prestige of the program is elevated by classifying all or portions of it. Even in a properly classified program, the "prestige" phenomenon may result in the decision to overgrade the information, or to establish an unnecessary special access program. Agency oversight is critical to curbing overclassification. Managers who do not demonstrate restraint in the classification process should be relieved of this critical responsibility.

(d) Disregard of the portion marking requirements of E.O. 12356 continues to be a problem. The Order requires all classified documents to be marked to indicate which portions are classified and the level of classification. While agency heads may waive the requirement in certain situations, portion marking is especially important for information that is transmitted outside the originating office or for information that serves as a potential source of derivative classification. While most agencies and officials adhere to the rules on portion marking, some continue to transmit classified documents that have no portion markings. A result may be the unnecessary proliferation of derivatively classified information.

Classifiers most often excuse their lack of portion markings on the basis that they are "too busy" to bother with them. ISOO does not accept this. The time saved by failing to portion mark in the first instance is lost over and over again by persons who subsequently must deal with the information. Moreover, the fact that most classifiers, including some of the highest level officials within the executive branch, find the time to portion mark their classified documents undermines those who choose to shirk this responsibility.

FY 1984 Program Weaknesses: Statistical

(a) Because increases in classification activity are generally viewed as something to be avoided, ISOO lists the 9% derivative classification increase in FY 1984, and hence the 9% increase in total classification activity, as a program weakness. However, this requires some explanation. It is becoming increasingly clear that the current build-up of classified defense and intelligence programs is almost exclusively reflected in derivative actions based upon classification guides. A classification guide identifies information to be classified in the interest of national security, and prescribes the level and duration of classification for each identified item of information. The military services and defense agencies, which already relied heavily upon guides, are issuing additional guidance to cover new programs and weapons systems. The CIA and FBI, which largely spurned the use of guides until recently, now rely on them for the bulk of their classification decisions. As recently as FY 1982, original classification accounted for 6% of total classification activity. By FY 1984, it was down to 4%. This reduction largely reflects a radical change in the way information is classified in the intelligence agencies outside the DoD.

Despite the greater numbers of derivative decisions, the increased reliance upon classification guides presents a clear opportunity for the executive branch to gain and maintain better control of the classification and declassification processes. The issuance of a guide is an original classification action that only an authorized original classifier may discharge. Because a single guide often initiates thousands of derivative classification decisions, it is imperative that its author(s) understand its consequences. Clear thought, analysis, and presentation within a guide offers accuracy, uniformity, and control over the classification and declassification of a significant quantity of information. As guides account for more and more of the classified product, assuring their quality has become a paramount concern of those responsible for the quality of the information security system itself.

(b) Despite statistical evidence that the systematic review for declassification program may be healing, the program remains a matter of great concern. The vitality of systematic review primarily depends upon the vitality of the program within the National Archives and Records Administration, the only agency required to conduct a program. Following expressed concerns about the health of the program by the Assistant to the President for National Security Affairs, the Archivist of the United States commissioned a study that recommended increased resources and revised procedures for the systematic review process. For FY 1985, NARA is now hiring or placing additional personnel on the program. Unfortunately, budget limitations have already wiped out any further increases for FY 1986. NARA's increased systematic review product may not be evident until then.

The establishment of NARA as an independent agency raises several questions about the future of systematic review. Chief among them will be the attitude of NARA's new top management to the program and their ability to gain increased resources. ISOO believes that a viable systematic review program, assuming the continued commitment of agencies not required to participate, depends finally on NARA being able to review approximately 10 million pages of classified documents annually. Achieving that level remains questionable.

Conclusion

In its second full year of operation, the information security system established by E.O. 12356 remained healthy and stable. There was widespread satisfaction with the system within the executive branch and little turbulence outside. Responsible officials and employees demonstrated greater familiarity with the system in FY 1984, and their performance generally reflected that knowledge.

At the same time, however, information security remains, as always, a vulnerable system. Its credibility is constantly subject to challenge, through unauthorized disclosures, unwarranted classifications, or otherwise. The system requires vigilance. It also requires the continued support of top officials from the President on down. The information security system under E.O. 12356 has received that support. It must continue to receive it.

Appendix

ISOO Inspections: FY 1983 and 1984

AGENCY FOR INTERNATIONAL DEVELOPMENT

- Bureau for Africa
- Bureau for Asia
- Office of Security

ARMS CONTROL AND DISARMAMENT AGENCY

- Office of Administration
  - Communications Section
- Strategic Programs Bureau
- General Advisory Commission on Arms Control
- Bureau of Multilateral Affairs

BOARD FOR INTERNATIONAL BROADCASTING

CENTRAL INTELLIGENCE AGENCY

- Directorate of Intelligence
- Directorate of Administration
- Directorate of Science and Technology
- Directorate of Operations
- Other Major Activities

CIVIL AERONAUTICS BOARD

COUNCIL OF ECONOMIC ADVISERS

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

DEFENSE COMMUNICATIONS AGENCY

DEFENSE CONTRACT AUDIT AGENCY

DEFENSE INTELLIGENCE AGENCY

- Directorate for Estimates
- Directorate for Scientific and Technical Intelligence
- Directorate for Intelligence and External Affairs
- Directorate for Communications
- Directorate for Foreign Intelligence
- Directorate for JCS Support
- Directorate for Research

DEFENSE INVESTIGATIVE SERVICE

DEFENSE LOGISTICS AGENCY

- Headquarters
- Defense Technical Information Center

DEFENSE MAPPING AGENCY

- Headquarters' Office of Security
- Office of Distribution Services
- Hydrographic/Topographic Center
- Special Security Office

DEFENSE NUCLEAR AGENCY

- Intelligence and Security Directorate
  - Counterintelligence Detachment
  - Classification Management Division
  - Security and Operations Division
- Radiation Directorate
- Shock Physics Directorate

DEPARTMENT OF AGRICULTURE

DEPARTMENT OF THE AIR FORCE

- Assistant Chief of Staff, Intelligence
- Assistant Chief of Staff, Information Systems
- Deputy Chief of Staff, Plans and Programs
- Deputy Chief of Staff, Research, Development and Acquisition
- Deputy Chief of Staff, Programs and Resources
- 1947 Headquarters Support Group - Air Staff
- Air Force Systems Command (Andrews Air Force Base)
  - Electronics Systems Division (Hanscom Air Force Base)
  - Aerospace Systems Division (Wright-Patterson AFB)
  - Foreign Technology Division (Wright-Patterson AFB)
- Air Force Logistics Command Headquarters (Wright-Patterson AFB)

DEPARTMENT OF THE ARMY

- Assistant Chief of Staff for Intelligence
- Deputy Chief of Staff for Operations
- Military District of Washington
- Criminal Investigation Command
- Comptroller of the Army
- Logistical Command
- Military Traffic Management Command
- Office of the Adjutant General
- National Guard Bureau
- Intelligence and Security Command
- Corps of Engineers
- Materiel Development and Readiness Command
- Missile Intelligence Agency, Huntsville, Ala.
- Ballistic Missile Defense Systems Command, Huntsville, Ala.
- U. S. Army Missile Command, Huntsville, Ala.
- Communications - Electronics Command, Ft. Monmouth, N.J.
- U. S. Army Natick Research and Development Command, Natick, Mass.
- Army Materials and Mechanics Research Center, Watertown, Mass.
- White Sands Missile Range, Las Cruces, New Mexico

DEPARTMENT OF COMMERCE

- Headquarters' Office of Security
- National Telecommunications and Information Administration
- International Trade Administration

DEPARTMENT OF EDUCATION

DEPARTMENT OF ENERGY

- Energy Information Administration
- Office of Classification
- Office of Computer Services and Telecommunications Management
- Office of General Counsel
- Office of International Security Affairs
- Office of Management and Administration
- Office of Security and Safeguards

DEPARTMENT OF HEALTH AND HUMAN SERVICES

- Office of the Secretary
- Food and Drug Administration
- National Institutes of Health

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

DEPARTMENT OF THE INTERIOR

- Headquarters' Office of Security
- U. S. Geological Survey
- Bureau of Mines

DEPARTMENT OF JUSTICE

- Federal Bureau of Investigation
- Immigration and Naturalization Service
- Drug Enforcement Administration
  - El Paso Intelligence Center
- Bureau of Prisons
- Foreign Claims Settlement Commission
- Main Justice
  - Antitrust Division
  - Civil Division
  - Criminal Division
  - Justice Management Division
  - Tax Division
  - Office of Intelligence Policy and Review
  - Office of Information and Privacy

DEPARTMENT OF LABOR

Office of Emergency Preparedness Planning (Information Security)
Bureau of International Labor Affairs
Bureau of Labor Management Relations and Corporate Programs

DEPARTMENT OF THE NAVY

Office of the Chief of Naval Operations
Naval War College, Newport, R.I.
Naval Underwater Systems Center, Newport, R.I.
Naval Underwater Systems Center, New London, Cn.
Naval Intelligence Support Center
Naval Research Laboratory
Joint Cruise Missile Project Office
Office of Command Control
U.S. Atlantic Fleet Headquarters, Norfolk, Va.
Commander Naval Surface, U.S. Atlantic Fleet, Norfolk, Va.
Headquarters Fleet Marine Force Atlantic, Norfolk, Va.
Commander Submarine Force, U.S. Atlantic Fleet, Norfolk, Va.

DEPARTMENT OF STATE

- Classification/Declassification Center
- Information Systems Office
- Information Systems Security Staff
- Office of Security
  - Domestic Operations
  - Education and Training Staff
- Bureau of Intelligence and Research
  - Office of the Executive Director
  - Office of Economic Analysis
- Bureau of East Asian and Pacific Affairs: Japan
- United States Mission to the United Nations
  - Office of Administrative Affairs
    - Reference Section
  - Political Section
  - Economic and Social Section
  - Communications Section
  - Security
  - Resources Management

DEPARTMENT OF TRANSPORTATION

Office of the Secretary
Federal Aviation Administration
United States Coast Guard (Headquarters, Miami, New Orleans)
Maritime Commission

DEPARTMENT OF THE TREASURY

- Office of the Secretary
- U. S. Customs Service
- Internal Revenue Service
- U. S. Secret Service
- Bureau of Alcohol, Tobacco, and Firearms
- Bureau of Engraving and Printing
- Bureau of Public Debt
- Bureau of Government Financial Operations
- Comptroller of the Currency
- Bureau of the Mint

ENVIRONMENTAL PROTECTION AGENCY

EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF ADMINISTRATION

EXPORT IMPORT BANK

FARM CREDIT ADMINISTRATION

FEDERAL COMMUNICATIONS COMMISSION

FEDERAL EMERGENCY MANAGEMENT AGENCY

FEDERAL HOME LOAN BANK BOARD

FEDERAL MARITIME COMMISSION

FEDERAL RESERVE SYSTEM

GENERAL SERVICES ADMINISTRATION

INTERNATIONAL TRADE COMMISSION

INTERSTATE COMMERCE COMMISSION

MARINE MAMMAL COMMISSION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

- Office of Aeronautics and Space Technology
- Office of Space Science and Applications
- Office of Space Flight
- Office of Space Tracking and Data Systems
- Goddard Space Flight Center
- John F. Kennedy Space Center

NATIONAL ARCHIVES AND RECORDS SERVICE

NATIONAL LABOR RELATIONS BOARD

NATIONAL SCIENCE FOUNDATION

NATIONAL SECURITY AGENCY

NATIONAL SECURITY COUNCIL

NATIONAL TRANSPORTATION SAFETY BOARD

NUCLEAR REGULATORY COMMISSION

- Office of International Programs
- Office of the Deputy Executive Director for Operations
  - Division of Security
  - Rules and Records Division
  - Records Services Branch
  - Standardization and Special Projects Branch

OFFICE FOR MICRONESIAN STATUS NEGOTIATIONS

OFFICE OF MANAGEMENT AND BUDGET

OFFICE OF PERSONNEL MANAGEMENT

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

OFFICE OF THE SECRETARY OF DEFENSE

- Under Secretary of Defense for Policy
- Assistant Secretary of Defense for International Security Policy
- Assistant Secretary of Defense for International Security Affairs
- Net Assessment
- Defense Guidance Staff
- Emergency Planning
- Assistant Secretary of Defense for Health Affairs
- Assistant Secretary of Defense for Legislative Affairs
- General Counsel
- Under Secretary of Defense for Research and Engineering
- Intelligence Oversight
- Assistant Secretary of Defense, Comptroller
- Assistant Secretary of Defense, Manpower, Installations and Logistics
- Assistant Secretary of Defense for Reserve Affairs
- Assistant Secretary of Defense for Public Affairs
- Inspector General
- Plans, Analysis and Evaluation
- Defense Security Assistance Agency
- Assistant to the Secretary of Defense for Atomic Energy

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE

OFFICE OF THE VICE PRESIDENT

ORGANIZATION OF THE JOINT CHIEFS OF STAFF

- Office of the Secretary
- Office of the Director, Joint Staff
- Office of the Chairman
- Manpower and Personnel Directorate
- Operations Directorate
- Logistics Directorate
- Plans and Policy Directorate
- Support Services Directorate
- Joint Analysis Directorate
- Command, Control and Communications Systems Directorate
- Joint Planning Staff for Space
- Strategic Plans and Resource Analysis Agency
- Joint Special Operations Agency
- United States Readiness Command, Tampa, Fla.
- United States Central Command, Tampa, Fla.

OVERSEAS PRIVATE INVESTMENT CORPORATION

PEACE CORPS

PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD

PRESIDENT'S INTELLIGENCE OVERSIGHT BOARD

SMALL BUSINESS ADMINISTRATION

UNITED STATES INFORMATION AGENCY

- Office of Security
  - Physical Security Division
- Office of American Republics Affairs
- Office of North African, Near Eastern, and South Asian Affairs
- Office of Public Liaison
- Office of Administration and Technology
  - Classified Library

UNITED STATES POSTAL SERVICE

- Office of the Chief Postal Inspector
  - Inspection Service

VETERANS ADMINISTRATION

THE WHITE HOUSE
WASHINGTON

April 29, 1985

Dear Mr. Garfinkel:

Thank you for your most recent report on the status of the system we have established under Executive Order 12356 to protect national security information. In that Order I entrusted the heads of our departments and agencies to provide better protection for this critical information while working to prevent unwarranted classification. I am very pleased to learn that our performance during the system's second year of operation has matched the impressive successes of its first year.

Your report notes the contribution of senior officials within this Administration in making the information security system work and calls for their continued assistance. I remain personally committed to the program's success. We must be unceasing in our efforts to halt those practices that threaten its effectiveness, including unauthorized disclosures and overclassification, and to strengthen those programs that provide the public with access to information that no longer requires protection.

I am grateful to you, your staff, and the other dedicated persons throughout the government who are working diligently on behalf of our national security. Your outstanding oversight activities must remain constant.

Sincerely,

Ronald Reagan

Mr. Steven Garfinkel
Director
Information Security Oversight
  Office
18th and F Streets, N.W.
Washington, D.C. 20405

STATEMENT SUBMITTED BY

DR. ROBERT E. LARSON

TO THE

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

HEARINGS ON

U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM

MARCH 1985

WRITTEN STATEMENT OF DR. ROBERT E. LARSON TO THE UNITED STATES SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

My name is Dr. Robert E. Larson. I am currently the Chairman and Chief Executive Officer of Visidata Corporation, a high-technology computer products company located in Fremont, California. On a volunteer basis, I have been extremely active in the Institute of Electrical and Electronics Engineers (IEEE), the world's largest technical professional society with over 250,000 members. I was a director of that organization for 7 years, vice president for technical activities in 1980 and 1981, and president in 1982. I have also been a consulting professor at Stanford University since 1973.

From April, 1968 to April, 1983, I was employed by Systems Control, Inc., a company I co-founded. I served on a number of positions in the company, including division manager, technical director, executive vice president, president, and chairman and chief executive office of Systems Control Technology, Inc., a wholly-owned defense-contracting subsidiary. During my employment with this company I worked on a number of important defense projects. I made major technical contributions in fields such as radar data processing, signal processing, missile guidance, including design of a special-purpose on-board computer for cruise missile guidance, advanced computer architectures for large-scale defense systems, command control and communication (C^3) networks and advanced ballistic defense systems. Since leaving Systems Control, Inc., I have done some additional defense work, including major contributions to studies associated with the Space Defense Initiative (SDI), especially in the area of battle management. I am proud to have contributed to the strengthening of our defense technology in this manner.

In 1979 and 1980, a most disturbing series of events took place. My executive secretary, Ms. Ruby Schuler, conspired with her husband, Mr. James Harper, to steal classified information from my company and to sell it to Polish intelligence agents. The damage inflicted by their actions to United States security is very grave, and I am personally very distressed about the entire episode.

The manner in which they carried out their efforts made it virtually impossible to apprehend them. Neither I nor anyone else in the company had any idea that a crime had ever been committed. Indeed the only reason for the discovery of their crime was that Harper attempted to negotiate a settlement with the FBI, through an attorney, in which he would be given immunity from prosecution in exchange for his disclosing all the information he knew. In may of 1983 I was approached by the FBI to see if I could help them establish conclusively the identity of the person negotiating the agreement. I was able to verify that the documents referred to in the correspondence were stored in my security safe, a safe to which Ms. Schuler has access. After several meeting with the FBI, we were able to deduce that the documents were taken from the safe, photocopied, and returned to the safe without anyone detecting them missing. This could easily be accomplished either by taking the documents home overnight and copying them there, or by coming in at night and copying them on an office copying machine. In any case, the matching of Harper's fingerprints to those on the backs of pages that had been copied was the conclusive evidence needed to indict Harper.

Ms. Schuler's background and demeanor gave no indication that she would ever be involved in such an incident. She came to work in the accounting department of Systems Control, Inc. quite early in its history. As one of the first 50 or so people in the company, she was in an excellent position for her career to grow as the company grew. After performing very capably as executive secretary to the head of our computer center, I hired her myself to help me track the financial operations of what was then the company's largest division. As my role in the company evolved she became my executive secretary. She performed very capably and adapted readily to new roles as my own position in the company changed. Throughout her career, she showed great loyalty to the company.

In about 1975, at a time when I was responsible for a major fraction of the company's defense work, she was given a security clearance at the secret level. Although she herself did no classified work directly, she did help me a great deal, both in filing and retrieving documents for my review and in typing documents I originated. It was very common for a secretary in her situation to be given a clearance. For a few years she has access only to the documents in my personal safe. Later, the security department at Systems Control, Inc., placed in my safe a large number of other documents that had been in the hands of an employee who returned to school on leave from the company. Unfortunately, this seemingly innocuous move resulted in her having access to a much larger set of documents when she decided to commit espionage.

Her one major personal problem was alcohol. She always had been a moderate to heavy drinker, but it didn't affect her work performance until about 1980. Unfortunately, by that time I was traveling extensively on business, both for the company and for IEEE, and I did not have a chance to observe her physical deterioration personally. During 1980 and 1981 I was out of the office more than 60% of the time, and during 1982 I was gone about 80% of the time. It was relatively easy for her to put in a good appearance on the few occasions I was in town, and no one in a position to observe her constantly told me of her condition until mid-1982. Before I could return to deal with the problem, she went on medical leave of absence. She died of cirrhosis of the liver in July, 1983, after the FBI was investigating her, with my assistance, but before Harper's indictment. It is my opinion that her sudden rampant alcoholism and subsequent death were due to a guilty conscience over the crime she had committed with Harper.

In examining this situation, it is difficult to see how to prevent crimes like this in the future. Thousands of people like Ms. Schuler have legitimate access to billions of pages of classified documents stored in safes and vaults around the country. With the widespread availability of copying machines, both in offices and in homes, it is hard to see how to prevent a repetition of this crime. The alternative of employing drastically more severe limitations in access to classified documents is not attractive either. The difficulty is how to balance national security against personal liberty and the operational efficiency of our defense industry.

It does appear that some reasonable safeguards can be taken. One approach is to use technology to try to prevent such crimes. For example, it might be possible to use recent advances in cryptography and computer security to store all classified data in encrypted form in a large computer storage facility and to restrict access via computer terminal very selectively to only those who need it. Although this solution may appeal expensive and not foolproof, the rapid trends toward office automation may soon make this idea quite realistic. Another approach is to print classified material on paper that would trigger a detection of some kind; it might then be possible to use surveillance on employees leaving the building to ensure that no documents are removed. Still another approach is to print classified documents on paper that cannot be photocopied. While I have not seriously investigated the practicality of these latter two ideas, it does seem worthwhile to fund some research into technological solutions to this problem.

A more straightforward way to safeguard classified information is to restrict access to classified documents to only those with a clear need-to-know. It is currently quite common practice for several people to share access to a tape, with little or no monitoring of their actions when they open it, with the result that any individual can quite easily take any document in the safe, whether it is appropriate or not. Perhaps a centralized facility could be established, operated by a highly reliable group of people, who are responsible for filing, retrieving, and typing documents and for controlling access to all this material. This facility could be supplemented by many small safes, each accessed only by an individual. The concept of a large central secure facility, operated by a small group of highly trusted people, supplemented by small safes with individual access, could prove to be both efficient and considerably more secure.

Another procedure that needs improvement is the system of random inspections of the contents of safes. Unfortunately, the timing of the "random" inspection is often well-known throughout the company, and there is ample opportunity to replace any documents that are being misused. Furthermore, the inspections are always during working hours. In the case of SCI, an overnight inspection might have discovered that Ms. Schuler had taken documents home for Mr. Harper to copy.

A most difficult issue to deal with is the idea of doing more investigation into people's background before they receive a clearance. The questions of individual privacy and the astronomical cost of in-depth investigations into all applications arise immediately. Certainly, nothing in Ms. Schuler's background would have prevented her from getting her original clearance. A more reasonable possibility would be to investigate people with a clearance periodically, say once every 5 years. Major changes in a person's situation, like Ms. Schuler's alcoholism, might be detected and provide a warning of a possible security risk.

Another possibility is to restrict more severely the number of people with clearances. Perhaps less clerical and support people who do not actually work with the classified information should be given clearance. Also people who do not use their clearances for extended periods of time could have them rescinded. If the process of obtaining clearances for people who clearly need and deserve them could be made more efficient and if more clearances for people who have only a marginal use for them could be rescinded expeditiously the result would be a more efficient and effective system.

It is noteworthy that the popular press is quite fascinated with espionage and tends to romanticize it. I recall vividly how excited Ms. Schuler was after reading The Falcon and the Snowman, a book about spying at TRW, Inc. in the early 1970's. While I doubt that this book alone caused her to become a spy, I can't help but wonder what the impact of such a book could be. Ironically, the book has been made into a movie that is very popular right now. Furthermore, a book is now being written about the Harper case with an eye towards portraying Ms. Schuler in a sympathetic light, such as Christopher Boyce is portrayed in The Falcon and the Snowman. It would seem that a public information program on the evils of espionage and the resulting damage to our country might be in order to counter this sort of portrayal.

Thank you for your attention to my comments. I would never have believed in my wildest dreams that I would become the victim of a spy ring, but it has indeed happened to me. Furthermore, there are all too many opportunities for it to happen again and again throughout the country. While I believe very strongly in the basic rights of individuals, and I recognize the need for large numbers of people to have access to classified data, I think that we can now change some of our procedures to improve security significantly without unacceptable disruption to individuals and the operations of the defense industry. I hope that this background information and these ideas prove helpful to your deliberations.

RESPONSE TO THE
SENATE PERMANENT SUBCOMITTEE
ON INVESTIGATIONS

INQUIRY
INTO

THE EFFECTIVENESS AND EFFICIENCY
OF THE GOVERNMENT'S
SECURITY PROGRAM AND
PERSONNEL SECURITY SYSTEM

LOCKHEED MISSILES & SPACE COMPANY, INC.
SUNNYVALE, CALIFORNIA

FEBRUARY 15, 1985

A. LOCKHEED MISSILES & SPACE COMPANY (LMSC) SECURITY PROGRAM

1. Program Basis - The LMSC Industrial Security Program is based primarily upon the contractual specifications of the Department of Defense Industrial Security Manual for Safeguarding Classified Information. Our programs intent is to prevent unauthorized access to classified information and to restrict access to unclassified information relating to classified contracts, prevent foreign access to advanced technology and materials, protect company and government property, and control access to company premises and security areas. This effort at LMSC applies to over 300 classified prime contracts being performed by some 24,500 employees. LMSC has 643 full-time professional security employees, about 50% of whom are members of a uniformed guard force. The Director of the Industrial Security & Safety organization oversees eight separately managed security organizations (See Attachment 1). The Director of Security and Safety, who functions under the staff supervision of the Director of Human Resources, has direct access to the President of LMSC. In addition to the professional staff, LMSC maintains a Security Coordinator Program, in which a security coordinator is assigned to each of the more than 800 functional organizations.

2. Industrial Security Program Fundamentals - LMSC adheres to fundamental management practices considered essential to an effective security program. They include the following:

a. Top Management Support and Participation - LMSC top management has always given complete support to security and has advocated and enforced compliance with security regulations at all levels. The company has a long standing procedure for handling security violations. This includes impartial investigation and a uniform system of penalties. These penalties range from written admonition or suspension to termination. Employees are made aware of this practice through comprehensive new hire orientations, annual refresher training, and demonstrated application. Annual security training sessions are regularly scheduled for all levels of LMSC Management.

b. Selection, Training, Motivation, and Supervision - An extensive and careful selection process is involved in the hiring of LMSC'S professional Security Representatives. These individuals provide the direct link between security and operating organizations. The majority of representatives are college graduates, some with advanced degrees. They have diverse security related backgrounds and expertise acquired in previous employment with the military, FBI, local law enforcement, and industry. New representatives attend a one week Defense Investigative Service (DIS) Industrial Security Course and a five week LMSC security training and orientation program. Security Representatives also attend regularly scheduled LMSC Security Professional Development Seminars. Security managers and supervisors attend the LMSC Management Institute or Supervisor's Institute (run in conjunction with University of Santa Clara). Security managers and supervisors also attend and participate in meetings and seminars of the Aerospace Industries

Association, the American Society for Industrial Security, and the National Classification Management Association along with numerous other government and industrial seminars and institutes. Information obtained at these meetings is widely disseminated to other security personnel.

c. Security Education - LMSC has a comprehensive and continuing security education program for all employees. Initally a new hire orientation covering mandatory DoD requirements, company procedures, and motivational information is presented. When an employee receives a security clearance, a detailed briefing on specific work related security is provided. Thereafter, the organization Security Coordinator gives each cleared employee on-the-job and annual security reindoctrination. Security Representatives advise, assist, and participate in this annual training. LMSC Security Representatives give individual training to each newly appointed Security Coordinator and provide necessary reference material. Security Coordinators attend annual refresher security training courses.

d. Communications - Various means of communication are used at LMSC for effective security administration. Information flows to the various organizational levels by means of weekly staff meetings and Highlight Reports. The Government Security organization also distributes a monthly Security Newsletter for each line manager and Security Coordinator to aid in the dissemination of pertinent security information to employees. Security information is also conveyed by means of Supervisory Bulletins, the Lockheed Star (company paper), management correspondence and the company public address system. Standard security references and changes are provided to users in the form of a Security Manual and Document Control Procedures Handbook. Individual copies of the DoD Industrial Security Manual are issued to specific individuals throughout the facility. Security prepares numerous plans and procedures for new and specialized activities.

e. Government Relationships - Maintenance of professional standards of integrity and particularly in matters of security an open and cooperative relationship with the Defense Investigative Service, the resident Air Force and Navy Plant Representative Offices and other government agencies is a fundamental tenet of LMSC Industrial Security.

B. LMSC SECURITY ORGANIZATIONS AND FUNCTIONS

1. LMSC Government Security, Program Security, and Special Access Security - Although separately managed, the LMSC Government Security, Program Security, and Special Access Security organizations perform substantially the same functions. These organizations differ in that while Government Security is primarily concerned with safeguarding classified information under DIS cognizance, Program Security and Special Access Security are responsible for proprietary and Sensitive Compartmented Information (SCI) activities. With a

total of 171 employees, these organizations are responsible for security procedures, training, compliance, and services for some 24,000 security cleared employees. Each organization is managed from central offices which provide company-wide services and direct operations of several supervised area offices. The central and area office clerical personnel perform conventional office duties as well as handling a large volume of detailed security paperwork. For example, in 1984 Government Security clerical personnel interviewed over 3,000 clearance applicants and processed their questionnaires, related records, and individual correspondence to the Defense Industrial Security Clearance Office. They also handled over 26,000 outgoing requests for classified visits and a similar number for incoming visits. They maintain individual security files for employees, consultants, resident contractors, and long term visitors. Facility clearance records are maintained for 365 classified subcontractors currently requiring access to classified information. Program and Special Access Security have similar functions and volume with additional specialized requirements for clearance applicant data and access authorization briefings. Security Representatives in each organization serve as the direct link between the security and operating organizations. These representatives perform a variety of routine and special duties, including:

a. Procedures requiring security representative approval, coordination, or briefing:

- o Admission of non-citizens to company premises
- o Use of privately-owned cameras or recorders on company premises
- o Handcarry of classified material via commercial aircraft
- o Visits to communist countries or attendance at meetings where communist country citizens may be present
- o Use of guards for classified meetings or security area escort
- o Public tours
- o Operation of classified computer areas and equipment
- o Establishment and operation of security areas
- o Access to Top Secret, Communication Security, Cryptographic, NATO, CNWDI (Critical Nuclear Weapons Defense Information) and other special categories of information

b. Other Security Representative duties:

- New hire orientation, Security Coordinator training, line organization training, and detailed briefings for special access approvals
- Security violation investigations, reports, and corrective action
- The periodic tracking of classified transmittals
- Conducting semi-annual company-wide security compliance inspections
- Providing guidance to managers and coordinators assuring security awareness and compliance
- Assist Department of Defense security inspectors during the formal two-week long semi-annual DIS program review and many other specialized customer inspections at LMSC
- Participate in physical security overviews of buildings and security areas
- Review vistor control procedures to assure that visitor clearances have been verified
- Issue instructions and monitor arrangements for classified meetings

c. Individually assigned Security Representative duties:

- Top Secret Control
- NATO information control
- Cryptographic/Communications Security
- Classified Hardware Control
- Monthly Newsletter preparation
- Management Procedures and Security Manual preparation and revision
- Monitor specialized Security Agreements with resident military and associate contractor groups
- Monitor control of Special Intelligence Material
- Computer Security
- Consultant administration

d. Security Areas - LMSC has over 130 security areas plus several conference rooms approved for classified uses. Security Representatives participate in construction planning of these areas which are built to meet DoD or SCI requirements and standards. Security Representatives issue special operating instructions for each area and monitor compliance.

e. Security Coordinator Program - To assure effective security administration within each of the more than 800 LMSC functional organizations, organization managers are required to appoint one of their responsible salaried employees the collateral assignment of Security Coordinator. The Security Coordinators are trained by Security Representatives and have broad authority for security matters within their organization, long tenure, and a high level of security knowledge and competence. They serve as a regular communications link between the line organizations and the full-time security staff. The Security Coordinator Program is indispensable to LMSC security.

2. Document Management - The Document Management organization is responsible for establishing procedures for control of classified material, operating stations, receipt and transmittal of documents, and maintainance of a system for internal document accounting. Material is moved within LMSC by security cleared mail and courier personnel via a network of 39 stations operated by full-time document control specialists. Individual organizations also have over 100 substations which assign employees to handle classified material. There are about 475,000 Secret signature accountable documents in the control systems which require approved storage and access. Document Management personnel also maintain separate accountability records and special handling for Top Secret, NATO, COMSEC, and consultant material. Managers provide written need-to-know certification for each employee permitted to receive classified documents. Personnel in the document stations average more than five years experience in their specialty.

3. Plant Protection - The Plant Protection organization is LMSC'S largest single security organization, employing 314 employees. This organization provides company-wide physical security services through four operating sections.

a. Uniformed Section - The Uniformed Section, which operates 24 hours a day, seven days a week, has three Shift Commanders, 11 Shift Captains, and 265 Security Officers. The typical Security Officer is 38, has completed at least one year of college, and has an extensive military or law enforcement background. New Security Officers receive comprehensive classroom training and must complete an 18 week probationary program. In addition to scheduled assignments, Security Officers perform special assignments such as classified meeting admission control and security area escort of visitors or construction workers.

b. Access Control and Alarm System (ACAS) Section - The ACAS section operates one of the largest proprietary burglar alarm systems in the country, with 2,477 alarms on three different systems. The ACAS system, in addition to the central command computer, includes four regional computers providing alarm functions and access controls for the facility. This sophisticated system couples magnetic card readings with personal identification codes to assure a high integrity personnel access control capability.

c. Locksmith Section - This section issues and controls all keys and locking devices used at LMSC . All are qualified locksmiths. There are 20,180 changeable combination security padlocks, 733 Safemaster door locks, 4,746 safes, 34 vaults, and 848 cypher locks, all of which require annual or semi-annual combination change. Employees in this section also establish coded key systems, maintain lock and key accountability, install lock cylinders, and open safes and locks which have malfunctioned.

d. Identification Section - The ID Section employees issue and control passes and badges for LMSC employees and non-employees, including the Air Force and Navy Plant Representative Offices. They take ID photographs and fingerprints, type required forms, and maintain records. During 1984, the ID Section issued 17,164 employee badges, 2,489 non-employee badges, 14,986 special badges, fingerprinted 8,775 security clearance applicants, and processed 4,790 employee clear-in-actions.

4. Investigation Bureau - The Investigation Bureau conducts inquiries into the following matters: Loss or damage to company or government property, violations of LMSC Management Polices or Directives, incidents of espionage or sabotage, offenses committed against the person or property of company employees occurring on company property or while the employee is on company time.

In addition, the Investigation Bureau conducts security prescreening of prospective employees which includes credit, education, employment, court records, and reference checks.

Prescreening provides a limited background check of prospective employees, especially those in the immediate geographic area.

5. Security Services - The basic responsibility of Security Services is to provide company wide security support in the areas of classification, computer security, security training media, technical and physical security. To accomplish this, Security Services is functionally organized to accomplish the following.

a. Classification Management - The principal thrust of security organizations is toward protecting classified documents and hardware. To protect information it must first be identified. The function of the Classification Management Office then, is to:

- Receive, interpret and disseminate contract classification specifications and classification guides issued in connection with classified contracts and proposals,

- Prepare classification specifications for all classified subcontracts,
- Monitor the performance and effectiveness of all LMSC Classification Management activities.

Some of the areas requiring Classification Management oversight, include:

(1) Requests for Proposals
(2) Proposals
(3) Contract definitions
(4) On-going programs
(5) Independent research & development
(7) Proprietary rights and interests
(8) Press releases
(9) Publications and speeches
(10) Technology transfers
(11) Export control
(12) Classified hardware surplus

The challenge is to match the information security desires and needs of the government to the capabilities of our corporation. Information that is unclassified and arbitrarily evaluated as classified will create difficulty of access as well as initiate costly administrative procedures for control, handling and storage. Classified information not properly identified and provided adequate safeguards can lead to serious consequences to the user, the company, and our national security.

Classification Management professionals work closely with the government contracting officers and company management to ensure the timely classification action required to fulfill our obligations under both the Information Security Program and the Industrial Security Program.

b. Computer Security Analysis Group - The Computer Security Analysis Group has responsibility for Information Systems security at LMSC and is responsible for establishing a computer security program to protect against the unauthorized use, modification or destruction of company data processing equipment and/or information. The tasks can be divided into three major functional areas: To advise and assist all LMSC personnel (to include security, program, data processing, and contract management personnel) relative to computer security matters, to provide guidance and coordination in the formulation of data processing policies and procedures as they relate to computer security, to conduct computer security assessments of LMSC's computing resources providing the basis for management decisions regarding computer security.

c. Security Training

Security Training designs and produces a variety of security training media and programs in the form of posters, video tapes, brochures, etc., for use in the ongoing company security education program. The training media are tailored to specific security needs and are used throughout the company by both security personnel and the line organizations as well as by our customers and by other Lockheed companies. This program has received widespread recognition and has won awards in national competitions

d. Technical Security - Technical Security is responsible for physical security, technical security, Tempest, alarms, access control, and locking devices. Technical Security ensures that facility modifications and construction meet customer security standards. The Technical Security Office is staffed with security professionals who have extensive backgrounds and experience with various U. S. Government agencies, and private industry.

Technical Security advises management regarding telephones, audio countermeasures, compromising electrical emanations, alarm systems, access control and locking devices.

C. COMMENTS ON THE EFFICIENCY AND EFFECTIVENESS OF THE DEFENSE INDUSTRIAL SECURITY PROGRAM (DISP)

The primary objective of the DISP is to safeguard classified information in the hands of industry. To accomplish this, the government enters into a contract (security Agreement) with a company in which the company agrees to abide by provisions of the DoD Industrial Security Manual for Safeguarding Classified Information. DIS briefs the company in ISM requirements and, thereafter, inspects the company for compliance, critiques company performance and issues letters directing corrective action when deemed necessary. The company responds by taking corrective action. This arrangement gives a company government support, stimulates employee concern for security, and assures that administrative security procedures are performed properly. It is a sound system, effectively implemented. It promotes security discipline and establishes boundaries of individual and corporate responsibility.

It is DIS policy to work in a "partnership" relationship with contractors; to provide advice, assistance and be available as consultants. The "partnership" approach has worked well for LMSC. Honest disagreements have been expressed without acrimony or repercussion. The long standing DIS policy that permits shaping government security requirements to a company's operations rather than changing operations to fit requirements has produced efficiency and sound security. The DISP provides a good baseline protective system for sensitive government information in the hands of industry.

The physical, administrative and procedural aspects of the DISP are quite adequate. The human reliability aspects need improvement. Much could be accomplished by better coordination and exchange of existing information between DIS and the various Federal law enforcement and intelligence agencies. Better security clearance reliability is achievable.

Guidance to industry in matters of human reliability and potential threats is lacking. Industry receives little information regarding the threats from terrorist groups or foreign espionage agents in the local area or the United States, as a whole. It does not seem to be DIS practice to obtain and make available domestic intelligence, counterintelligence, and human reliability information collected by the FBI and other intelligence activities. DIS investigators become privy to such adverse intelligence information regarding company employees but even when any employee's clearance is revoked, the company is not informed of the basis. Advice, assistance and government cooperation is in greatly needed in the area of human reliability.

D. COMMENTS ON THE RECOMMENDATIONS OF THE DEFENSE INDUSTRIAL SECURITY REVIEW COMMITTEE

1. Increased Emphasis on Counterintelligence and Human Reliability within the Defense Industrial Security Program

We believe DIS should, with careful consideration, increase efforts in human reliability and counterintelligence. In the past DIS efforts have been almost entirely devoted to administrative inspections. This type of inspection is hardly likely to expose a Christopher Boyce or a James Harper. Industry must look to DIS for guidance. DIS in turn should have an active and productive liaison with national intelligence agencies to obtain the basis for this guidance. Excesses and poor judgement in implementing a human reliability program could result in public criticism and claims of privacy invasion.

A properly managed DIS hostile threat briefing program would be welcomed. Past experience has shown that presentations by either US government representatives or industry representatives with recent direct involvement in significant espionage, connterespionage or technology transfer cases are particularly well received. Presentations should do more than merely reiterate case histories already presented by various media. At the same time, it should be remembered that some material presented to and discussed with corporate security management might not be appropriate for all audiences. Audience-tailored briefings would be advised.

2. Priority Emphasis on Security of Sensitive Contracts

An effort to focus special attention to the most sensitive contractor facilities could attract undue attention to the very programs DoD is attempting to shield from disclosure.

3. Revision of the Industrial Security Manual

The Industrial Security Manual establishes base line protection for the sensitive information entrusted to over 13,000 contractor facilities in the DISP. While simplification is a worthy goal, consistent guidance is equally important. Much of the detail is not inordinate but necessary to prevent multiple interpretations of the requirements. The evolution of these details have for the most part, come from the cooperative efforts of government and industry.

4. DIS Inspection of Special Access Programs

We believe that DIS should provide training support and professional staffing to user agencies at their request. Supervision of the contract should remain the prerogative of the user agency.

5. Strengthening the Adjudication Process

The recommendation for uniformity is certainly favored by industry.

Consistent adjudicative standards should be applied to all individuals being considered for security clearances and access authorizations. All adjudicators should follow the same guidelines. Program and agency variations should be eliminated.

6. Centralization of the Adjudication Function within the Department of Defense

Security clearances and access authorizations are the result of administrative actions. Subjects of these proceedings within industry voluntarily participate. The issue of the use of subpoena power requires further study. It is our understanding that the government can obtain the necessary information under the contract.

7. Revising the Frequency of the Industrial Security Inspections

We concur with the establishment of an inspection system that considers the volume and complexity of classified activity in establishing frequency of inspection.

8. Reporting of All Foreign Travel by Contractor Personnel

We concur with this recommendation under the following conditions:

a. Reporting be made a government requirement for all cleared employees.

b. Unusual cases reported to DIS by industry must receive prompt and serious attention.

9. Creation of Separate Advisor and Inspector Roles of DIS Representatives

The present system is adequate. The creation of separate roles for DIS representatives would be inefficient and would decrease productivity.

10. Establishment of a National Industrial Security Hotline

The potential for misuse and abuse of a Security Hotline cannot be ignored. There are ample alternative methods for reporting suspected cases of espionage via local FBI or Regional DIS offices. The Security Hotline is strongly discouraged.

11. Assignment of DIS Personnel to Extremely Complex or Particularly Sensitive Contractor Facilities.

We disagree with the recommendation that DIS representatives be assigned to an extremely complex or sensitive contractor facility. This would duplicate the existing DIS organization, already responsive to contractor needs. It would be virtually impossible for one person to have the expertise and facility familiarity to serve effectively. These types of facilities normally have professional security staffs that have equal or greater expertise than the DIS personnel.

12. Establishment of a Graded Defense Industrial Security Program Inspection Rating System

The present inspection rating system has worked satisfactorily for many years and is used by other government agencies. It is difficult to envision a graded system that would be objectively administered. Methods currently exist to recognize outstanding overall performance and special achievement.

13. Specialized Training Program for Accrediting Contractor Security Personnel

The present DIS ISM training program is very good. An actual certification of proficiency would represent a Government judgement of skill to perform a company function. We do not believe this appropriate or necessary. Industry welcomes other means to augment employee training.

14. Notification of the DIS of Criminal Investigations Involving Cleared DoD Contractors and Contractor personnel

We support the notification of DIS of criminal investigations involving cleared DoD Contractors and Contractor personnel and encourage the availability to DIS of other federal data base material.

15. Legislative Base for the Defense Industrial Security Program

We support the establishment of a working group to draft legislation that would carefully address the problems in the prosecution of espionage cases.

16. Legislation to Limit Administrative and Judicial Review of DoD Personnel Adjudication to the Adjudicative Procedures themselves

We support a study of legislative initiatives to limit administrative and judicial review of DoD personnel security adjudications as long as particular attention is given to the individual's constitutional guarantees.

17. Authority to Suspend and Debar Contractors for Serious Security Infractions

Each case must be reviewed on an individual basis. There must be a recognition that the actions of the individual do not necessarily reflect the security awareness and practices of an entire corporation.

18. Revised Scope of Personnel Security Investigations

a. We agree with the recommendation that subject interviews be considered for incorporation as a part of the minimum investigative standards for the SBI.

b. We disagree with the recommendation to delete neighborhood and educational checks/verifications. We feel they assist overall evaluation of individuals elegibility for access to classified material.

19. Enhancement of Parsonnel Security Investigative Standards and Reduction of Industrial Clearances

a. Given the strain on the existing resources at DIS, we encourage the prioritization of periodic reinvestigations based on established criteria.

b. At this time, we do not have sufficient data to respond to this recommendation.

c. We support this recommendation. There are situations within industry when certain individuals require one-time or occasional access to classified information at one level higher than the personnel clearance currently in effect.

d. The submission of appropriate documentation to DISCO subsequent to the granting a of company-Confidential clearance is supported.

e. It appears the intent of the recommendation is to reduce the number of clearances and consequently the administrative burden. The implementation of an automatic expiration would increase DISCO's work load. This increase would be caused by the recertification of expired clearances.

f. We support the effort to streamline the administrative process by removing the requirement for contracting officer approval for all interim clearance actions.

g. The implementation of an automatic expiration would increase DISCO's work load. This increase would be caused by the recertification of expired clearances.

h. We support the recommendation of periodic reinvestigations on Secret clearances every five years. This should not be implemented, however, at the expense of the current intial investigation process. We do not wish to create a greater delay in the granting of clearances.

i. We agree that controls are needed to preclude frivolous clearance requests but disagree that to accomplish this an additional administrative burden be placed on DISCO. We encourage a requirement that industry maintain an internal system for clearance justification.

j. At this time, we have insufficant data to provide a value judgment on the relative merits of a counterintelligence questionnaire.

20. Documentation in Standard Practice Procedures Relating to Disciplinary Action for Security Violations

We concur that Contractors establish policy for the disciplinary action to be taken against an employee involved in Security Violations when culpability is established.

21. System of Controls over after-hours Access and Reproduction Equipment at Cleared Facilities

Although specific measures would enhance the protection of classified material, they would not be particularly effective in preventing or deterring espionage by a properly cleared individual with legitimate access. Many of the proposed measures are good as facility management techniques and should be encouraged for voluntary installation and for implementation as deemed appropriate by facility security personnel.

22. Access to the Defense Technical Information Center Classified Data

We concur in the need for stringent control of the Center's data. However, responsiveness to the needs of industrial and government researchers must be considered.

23. Proactive Efforts by the DIS to prevent Unauthorized Disclosures

There is now in place within the DISP a well defined mechanism for the review of data for public release via the contracting activity involved.

24. Increased Emphasis on Classification Management

There must be a greater emphasis on classification management within government. Since the object of industrial security is to safeguard classified information, it is critically important that sensitive information be adequately identified to assure the proper degree of protection is applied.

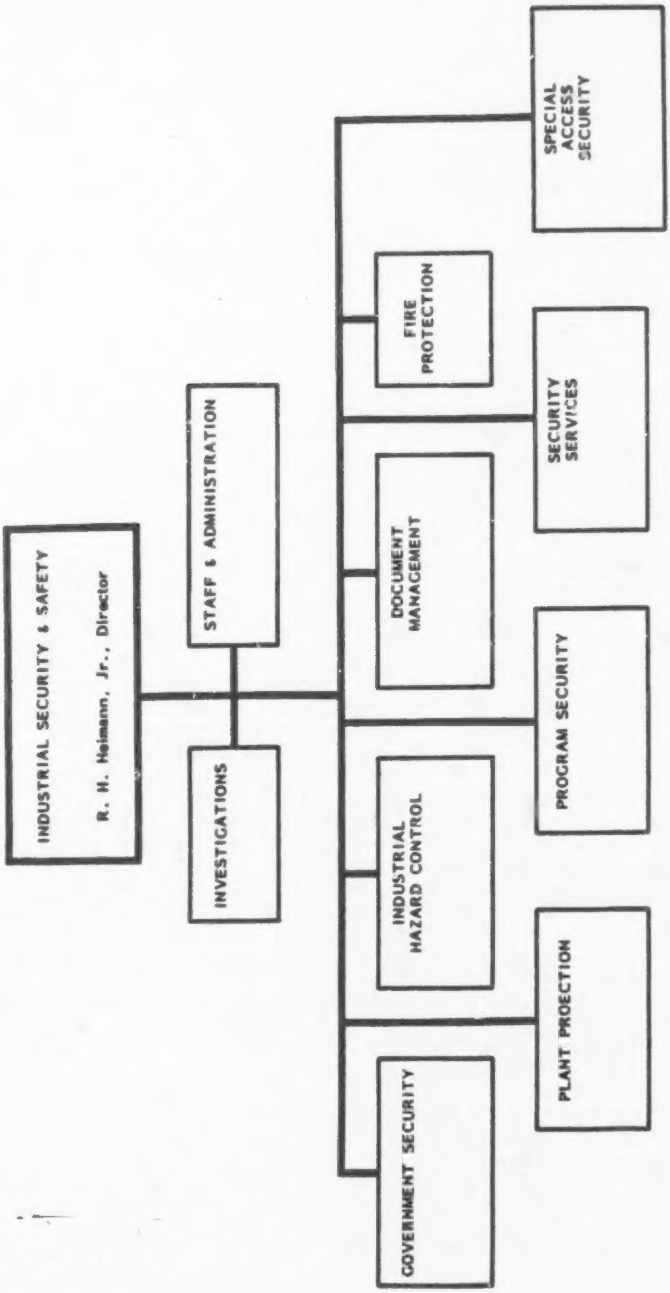
25. Prevention of "Bootlegging" of Classified Material

Additional measures do not seem necessary. Upon employment termination, each cleared employee signs a Security Termination

Statement, which states all classified material has been turned-in. Normal practices also require that management assure that all classified material is returned prior to an employee's termination.. Company indoctrinations cover the prohibition of unauthorized removal of classified material from the facility.

E. SUGGESTIONS FOR LEGISLATIVE OR REGULATORY REFORMS

We have no specific recommendations for statutory reforms, however, we favor legislation which would facilitate federal investigative agency access to information controlled by individual state laws required in investigations of personnel suitability for classified access. It is also believed that there may be legal barriers which prevent the denial or revocation of clearance for individuals that should not be entrusted with sensitive government information.


INDUSTRIAL SECURITY & SAFETY
R. H. Heimann, Jr., Director
INVESTIGATIONS
STAFF & ADMINISTRATION
GOVERNMENT SECURITY
INDUSTRIAL HAZARD CONTROL
DOCUMENT MANAGEMENT
FIRE PROTECTION
PLANT PROECTION
PROGRAM SECURITY
SECURITY SERVICES
SPECIAL ACCESS SECURITY

Lockheed Missiles & Space Company, Inc.

1111 Lockheed Way, Sunnyvale, California 94086

COMPARATIVE STUDY

PROPRIETARY VS CONTRACT GUARD SERVICES

Lockheed Missiles & Space Company, Inc. has considered the relative merits of contract vs. proprietary guard service over a number of years. Consequently, some of our facilities are protected by contracted guard forces and some by proprietary forces. The selection is generally determined by the quality of service required, the limitations on personnel turnover demanded by the operational requirements of the particular facility, the relative cost of the alternatives, as well as Collective Bargaining considerations. These four issues will be addressed in turn.

I. QUALITY CONSIDERATIONS

If costs were the only factor to be considered, contract guard forces might be the preferred method of providing guard services for our facilities. However, this is rarely the case. At its primary facility in Sunnyvale, California, Lockheed Missiles & Space Company, Inc. utilizes a proprietary guard force. This is due, in part, to the fact that LMSC is involved with some of the nation's most sensitive defense contracts which require a security guard force that is extremely reliable and exceptionally stable. The number and sensitivity of classified programs at LMSC requires that each of our officers be processed for a Top Secret security clearance based upon a Special Background Investigation. In addition, many security officers are asked by the government to submit to polygraph examinations. This clearance process averages eleven months to complete. While not every guard post requires a Top Secret clearance, most do and all require at least a Secret clearance. The posts with lower level clearance requirements provide for the productive utilization of those newer officers awaiting higher level clearances. In addition to being able to pass the most stringent government background investigation, LMSC officers must have the ability and training to properly respond to threats that could cause exceptionally grave damage to national security.

When considering "equivalent" or "comparable" contract guard service, it must be understood that, of the total guard service provided by contract nationally, only a fraction is utilized in cleared defense plants. And only a small portion of them are devoted to protection of highly sensitive activities. The great majority of contract guard service is devoted to strictly commercial activities such as retail stores, warehouses, sporting events, manufacturing, parking lots, etc. The personnel recruited into the commercial protection business are often those willing to work for very low wages, such as students or retirees seeking supplemental income, individuals between normal career jobs and others with various short-term employment goals. Guard service contracts normally do not exceed one year and a change of contractors each year is commonplace. All of this tends to produce a transient, inexperienced workforce with a low level of training and a limited interest in the task at hand.

It is not coincidental that most defense contractors with high-level security requirements elect to maintain their own proprietary guard force. It is very difficult and often impossible to contract for a high quality guard force with a low turnover rate. There are, of course, activities with high level security requirements that do contract for their guard forces. For example, certain DoE and DoD facilities with high security requirements have apparently been successful in contracting for guard services. However, two important factors must be noted when evaluating that success. First, these facilities often utilize both contract and employee guards with the contract guards being restricted to the peripheral posts and the higher paid employee guards handling the highly sensitive or critical duties. (This approach would not be feasible for LMSC; the existence of non-sensitive peripheral posts for employees awaiting higher security clearances is vital to continued operation). Second, these sensitive DoE and DoD facilities do not contract for guard services at average contract guard industry rates, as discussed below under "Cost Considerations".

II. STABILITY

Presently, the contract guard industry is undergoing explosive growth in providing service to the general business sector. In 1980, 54% of all guards were contract personnel. It is projected that by 1995 69% will be contract guards. Consequently, the contract guard service industry is undergoing serious growing pains. The leading problem associated with this growth is the high turnover rate in both guards and their management. It is not uncommon for a contract guard to work for three or more contract guard firms within a single year. Management fares no better, as evidenced by one major firm which changed its local management staff several times within a single year. The contract guard turnover rate has been quoted to be from as high as 200% by Timothy J. Walsh, in Protection of Assets to a relative low of 100% to 150% in various "Security Management" publications. None of these turnover rates could be tolerated by LMSC or its customers. Presently, the annual turnover rate in the LMSC employee guard force is 6.6% and has been historically very low.

David Berger in his 1979 textbook Industrial Security explained that the high turnover rate in the contract guard industry is a function of pay scales. The wages and benefits in the contract guard industry are not high enough to attract and retain qualified personnel and are, in fact, aimed at those who, for whatever reasons, are willing to accept very low wages for some limited period of time.

The contract guard companies also generally practice front-loading. More experienced officers are placed in a new client's company in the beginning of the contract and then gradually replaced with newer, less experienced officers. This exodus of experienced personnel results in a lower quality product than anticipated.

In addition to low pay, the high turnover rate of contract guard personnel has been attributed to lack of status within the client company, lack of any advancement prospects, lack of management backing and poor supervision.

As previously noted, the contract guard industry has a poor reputation for stability and adequate service. In a recent publication of "Security Management", James T. McBride, Quality Assurance Manager for Burns International Security Services, Inc. made the following points about the contract guard industry.

> "INADEQUATE STAFFING TECHNIQUES"
>
> "Perhaps the single greatest cause of agency replacement is guard turnover . . .excessive turnover seriously jeopardizes the security of the client's facility."
>
> "INADEQUATE TRAINING"
>
> "Guard training is one of the more controversial topics in the security industry, and perhaps rightly so, since some guard agencies simply don't bother to train their employees. In other cases, the training administered is substandard."
>
> "POOR QUALITY CONTROL"
>
> "The failure of guard company management to build the basic principles of quality control into their operations has been one of the major weaknesses of the industry, and has no doubt contributed to many a cancelled contract over the years."

III. COST CONSIDERATIONS

The claims of lower cost made by the advocates of contract guard services require closer scrutiny. Illustrated below is 1983 data reflecting the average pay scales for guards. It should be noted that the Guard I classification is primarily a warehouse night watchman function while the Guard II classification is that of a multi-tasked plant protection officer. This study by the U. S. Department of Labor, Bureau of Labor Statistics, pointed out that the rates of pay for employees classified as Level II guards are, on the average, 18.1% higher than those employees classified as Level I guards for manufacturing concerns. The study also reveals that the rates of pay for Level II guards employed by manufacturing firms are 38.0% higher than those employed by non-manufacturing firms.

		Average Straight-Time Earnings		
Occupation	Total # of Workers	All Industries	Manufacturing	Non-Manufacturing
Guards (total)	236,427	$ 5.05	$ 8.89	$ 4.49
Guards I	195,980	4.77	8.52	4.27
Guards II	26,698	7.42	10.06	6.52

Source: BLS Publication: Summary 84-3; Occupational Earning in All Metropolitan Areas; July 1983

In order to focus on the difference between in-house guard service cost and the expense of contracted security services, LMSC's compensation rate for Security Officers was compared to various contract guard service billing rates. (NOTE: LMSC's compensation rate for Security Officers as of 12/1/84 includes Average Base Rate of $11.57, COLA of $.32 and Fringe Benefit Cost of $3.91). Since some of these facilities are located outside the Bay Area, we also adjusted LMSC's compensation rate of $15.80 by the wage differential between the San Jose labor market and the respective facility's local labor market. This adjusted rate was then compared to the billing rates charged by the contract guard forces to the respective companies.

Facility Name	Billing Rate	LMSC Rate(1)	LMSC vs Billing Rate	Relative Pay Levels San Jose(2) vs Others	Relative Adjusted LMSC Rate	Relativ Adjuste LMSC vs Rate
LA Air Force Station, CA	$15.00	$15.80	5.3%	95.9%	$15.15	1.0%
Sandia Labs, CA	14.23	15.80	11.0	100.0	15.80	11.0
Rancho Seco, CA	14.17	15.80	11.5	91.8	14.50	2.3
Air Force Satellite Control Fac., CA	17.71(3)	15.80	(10.8)	100.0	15.80	(10.8)

1. Average Base Rates $11.57 & COLA $.32 & Fringe Benefit cost $3.91=$15.80.
2. U. S. Department of Labor, Bureau of Labor Statistics Extracted from Labor Relations Review 3/17/83.
3. Estimated billing rate based upon known Average Base rate of $13.62 plus 30%.

For example, LMSC's compensation rate is 11.0% above the billing rate being charged to Sandia Labs at their Livermore, CA facility by their contract service; since both organizations are located in the general San Jose Area, there has been no adjustment made to LMSC's base rate. By contrast, LMSC's unadjusted compensation rate is 11.5% above the billing rate charged to the Nuclear Power Plant, Rancho Seco, CA located near Sacramento, CA. But when the difference in wages between San Jose and Sacramento labor markets is taken into account, the actual premium paid by LMSC is only 2.3% above Rancho Seco's billing rate. Further, these statistics do not reflect recent cost-favorable changes in LMSC's Security Officers Collective Bargaining Agreement, such as our practice of hiring new guards at a $6.60 per hour base rate.

IV. LABOR CONSIDERATIONS

LMSC's proprietary guard force is represented by the International Association of Machinists and Aerospace Workers.(1) The present Collective Bargaining Agreement was effective December 4, 1983 and has an anniversary date of November 1, 1986. To procure a contract guard service during the life of the collective bargaining agreement may cause one or more counter actions. The first possibility is a grievance action. The second could be charges filed with the NLRB alleging unfair labor practices. The third might be breach of contract litigation. Remedies may include a "cease and desist" order and a return to the status quo.

NEGOTIATION OF A CONTRACT GUARD AGREEMENT DURING IAM&AW CONTRACT NEGOTIATIONS

In the 1983 contract negotiations with the IAM&AW, the Company was successful in negotiating a substantially lower minimum wage rate for security officers. The 1983-86 Agreement does not include a general wage increase - only lump sum wage supplements each year. This was less than the main (production and office) bargaining unit received wherein they were granted a third-year general wage increase of 3%. The contract was ratified by a very slim majority of the security officers.

The Agreement does not provide for any contract guard services nor does it preclude it. Contracting out is, however, a mandatory subject for bargaining. Though the company could bargain to an impasse, our Labor Relations management and staff firmly believe an attempt to contract out any portion of guard services would result in a work stoppage. A strike over this issue might provoke bitterness and dissension which would be virtually irreparable. It could have an adverse effect upon the performance of security duties within the bargaining unit. Dissension would create severe difficulties in the integration of contractor personnel with the LMSC employee guards.

An alternative to contracting for guard services at lower wage rates would be to attempt to maintain competitive wage rates with the collective bargaining unit in the future by holding the line on negotiating lower rates. It is extremely unlikely that a "take-away" in across the board wage rate cuts or a modification or elimination of cost-of-living (COLA) increases could be negotiated without resulting in a work stoppage. The Union has stated, with great conviction during the most recent negotiations, that such proposals would result in a strike. It is impossible to predict whether a long strike would result in a favorable outcome or if the impact of a long strike would be acceptable to our government customers.

CONTRACTING OUT DURING THE LIFE OF THE COLLECTIVE BARGAINING AGREEMENT

Grievance Action

Although LMSC may be able to successfully rebut an unfair labor practice charge if it contracts out for guard services, a challenge through the grievance procedure may be more difficult to overcome. It is highly probable that the Union would grieve any decision to contract out for guard services. If the grievance proceeded to arbitration, it is judged that there would be a better than 50-50 chance that the Union position would be sustained considering the following:

- There is no past practice of contracting out any guard services at the Sunnyvale Plant.

- Contracting out guard services would impact the integrity of the bargaining unit and effectively nullify the Collective Bargaining Agreement. The only classification in the bargaining unit would be either reduced or eliminated altogether. If all guard services are contracted, thereby eliminating the classification, there would, obviously, no longer be any need for the bargaining unit itself.

- There would be a serious impact on employees laid off as a result of contracting out. Since there is no other classification in the Collective Bargaining Unit, no internal transfers can be made within the unit. Displaced guards might be hired by LMSC into other positions, but this would be without seniority. Many of the guards would not be qualified for other jobs at LMSC because of the highly technical nature of those positions. Only lower paying entry level positions might be available.

- Although the contractor guard firm might hire some of the displaced guards, it would be without seniority and would involve the loss of certain benefits including the Lockheed Retirement plan. The practicality of laying off an employee, then having the same person hired by a contractor to do the same work at the same location and at lower pay is questionable. An employee in this situation, of facing extreme economic hardship may not be the loyal, diligent employee that LMSC's customers desire for the critical function of plant protection. An arbitrator would probably give much weight to the economic impact of laying off employees and having those persons rehired at a lower rate.

- Permanent work is being contracted out, not just work of a temporary duration, thus eroding the permanent bargaining unit, which would not be in the case in contracting out to meet temporary fluctuations in the work force due to brief periods of work overload.

- The guard work would continue to be performed on LMSC premises. It is not a question of sending limited work off the property.

- The only reason for contracting out in this case is to reduce labor costs, not because of the ineffectiveness of the present security force. LMSC's position would be far stronger if it had other legitimate purposes for contracting out, in addition to labor cost savings.

NLRB Considerations

The decision whether to contract for all or part of the security services, where driven by economic considerations, is a mandatory subject of bargaining under current labor law.(2) Therefore, before LMSC can make a final decision to contract for guard services, the current parties must bargain in good faith to impasse (although they do not have to reach agreement).

If the parties reach an impasse and the guard services are contracted out, the Union's recourse would be to file charges with the NLRB alleging an unfair labor practice in violation of the National Labor Relations Act.

LMSC however, should be able to successfully withstand such a challenge because of the following factors:

- The present Agreement does not specifically preclude contracting out.
- The "management rights" clause basically reserves all rights except those expressly limited or relinquished.(3)
- There is no language in the recognition clause which would preclude contracting out.(4)

Breach of Contract

The Union might also file a civil law suit alleging a breach of the Collective Bargaining Agreement. This can only be done after the remedies available under the Agreement have been exhausted. Such a suit would have a good chance of success when considering the same factors discussed above. The court may order specific performance restricting LMSC from contracting out for all or any of the guard services.

V. SUMMARY

Lockheed Missiles & Space Company, Inc. utilizes a proprietary employee guard force at its Sunnyvale, California facility because it needs a guard force that is unusually reliable and stable. The government requirement of high level security clearances and access authorizations makes contracting out for protective service particularly difficult. LMSC believes that its proprietary guard force has done an excellent job of protecting highly sensitive national defense materials for over 25 years. That quality of service would suffer greatly if LMSC were to utilize a contract guard service. Even if the quality were comparable, the pay differential is not significant and would offer little gain. Finally we would anticipate major labor disruptions and serious legal challenges if we were to contract out. Such disruptions would not be isolated to the security guard members of the IAM&AW, but would include sympathetic response from the other 7000 members of the union. At this time, we feel it would not be a sound business decision to contract for guard services.

04 Jan 85

Footnotes

(1) International Association of Machinists and Aerospace Workers, Missile and Electronic District Lodge 508 and Plant Protection Local Lodge 2231 (Santa Clara County Plant)

(2) Fibreboard Paper Products Corp. vs. NLRB 379 U.S. 203 (1964); Milwaukee Spring Division of Illinois Coil Spring Company 1983-84 CCH NLRB P 16029 (1984); Otis Elevator Company 1983-84 CCH NLRB P 16181 (1984)

(3) Article I, Section 6, of the IAM&AW and LMSC Plant Protection Local Lodge 2231 Agreement

(4) Article I, Section 2, of the IAM&AW and LMSC Plant Protection Local Local 2231 Agreement

Selected Bibliography

Berger, David Industrial Security, 1979

Walsh, Timothy J., author/editor, Protection of Assets, Vol I, Sec. 9, Parts 1-5, 1984

Butler, William G., "Asking the Right Questions", Security Management, March 1981

McBride, James T., "Why Guard Firms Lose Jobs", Security Management, Sept 1981

Kmet, Mary Alice, "Guard Industry Checkup: Staying Fit in the 1980's", Security Management, Sept 1981

Kingwell, Robert G., "What Lies Ahead", Security Management, Sept 1981

Clark, Roger C., "Stop the Revolving Door", Security Management, May 1982

Kent, James M., "Coexisting With Your Guard Contractor", Security Management, Nov 1983

STATEMENT FOR THE RECORD

OF

PHILIP T. PEASE

DIRECTOR OF SECURITY

NATIONAL SECURITY AGENCY

BEFORE

THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,

SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

Personnel Security at NSA

Foundation

Public Law 88-290 (50 USC 831-835) March 1964, states that no one may be employed in, detailed or assigned to NSA, or have access to classified information at NSA, unless it is clearly consistent with the national security.

This along with the current intelligence executive order - E.O. 12333 - and various directives of the DCI and the Secretary of Defense provides the foundation for NSA's personnel security programs. The relevant section of the executive order states that NSA's responsibilities include:

> Protection of the security of its installations, activities, property, information and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary.

Congress provided NSA this security legislation (Public Law 88-240) following two very harmful incidents in the early 1960s: the defection of two Agency employees to the Soviet Union and the espionage activities, on behalf of the Soviets, by a military person assigned to NSA. These cases showed shortcomings in NSA's security programs and have remained a constant reminder to the Agency of the reality of the foreign intelligence threat and the danger posed by disaffected, disloyal, unsuitable persons seeking, or holding, access to most sensitive information.

Since that time, the NSA Office of Security, and other elements involved in the security process, have generally received the resources needed to run a sound and extensive security program. These programs have the active support of the Director NSA and Agency management.

Personnel Security Programs

Personnel security programs are developed and carried out by the NSA Office of Security in cooperation with NSA's Personnel and Medical Directorates, Agency supervisors, contractor security officers and indeed all affiliates, civilian and military. There are specific personnel security programs for applicants for employment, contractor personnel, military personnel selected for assignment to NSA, and for continued security assurance of cleared, on-board affiliates.

There are certain requirements common to all categories of personnel seeking affiliation with NSA:

* Polygraph interview
* Special background investigation

- Clearance adjudication
- Indoctrination

And there are various programs directed at on-board, cleared personnel including:

- Security education and awareness
- Periodic reinvestigation (to include counterintelligence scope polygraph)
- Supervisory awareness

Highlights of some of these programs are described later in this paper.

A description of the security processing of applicants for employment follows to illustrate how a number of personnel security techniques are used and various elements of NSA cooperate in personnel security programs.

* An applicant is interviewed by a recruiter from the Office of Civilian Personnel. Security requirements are explained to applicant; the applicant submits biographic data.

* The applicant is interviewed at NSA by the Medical Directorate (psychological tests, psychological interview, physical), potential employing elements, and the Office of Security. The security interview is with the aid of the

polygraph. The polygraph interview confirms the applicant's identity and the truthfulness of the biographic form and its declarations; suitability and loyalty questions are asked, explained and discussed. Suitability questions include commission of crimes and drug abuse. Loyalty questions concern espionage, sabotage, and clandestine contacts. The questions are based on DCI personnel security standards and guidelines (DCID 1/14).

* If the results of medical, personnel and security processing raise doubts as to continued processing of the applicant, the relevant information may be reviewed by a joint panel of medical, personnel and security managers. This joint panel is an outgrowth of the aforementioned security disasters of the early 1960s. The follow-up inquiries showed that relevant information on applicants - that could have led to turndown of applicants - was not being shared between the security, personnel, and medical directorates. Now all information that could bear on clearance and employability is shared.

* A special background investigation (SBI) is then conducted (if the applicant remains in processing) by the Defense Investigative Service (DIS) or, in a modest number of cases, the NSA Office of Security. Together with the results of national agency checks (FBI and other records) this information is evaluated and sent to the aforementioned joint panel, if necessary.

* The Office of Security conducts a day long security indoctrination of all new employees covering such topics as: foreign espionage, NSA policies on foreign travel and associations, drug policies, need for prompt reporting of potential or actual security problems. At the end of that session the employee signs the NSA Security Agreement (a "nondisclosure agreement").

We emphasize again that all our affiliates are polygraphed, the subject of an SBI, adjudicated and indoctrinated: civilian applicant, contractor, military assignee, GSA, consultant. There are of course variations in the processing steps; and, military personnel receive much of their security processing under the auspices of their own service before arriving at NSA.

The Office of Security personnel involved in these personnel security activities are carefully selected and well-trained. While, as noted, NSA currently conducts only a minority of its own background investigations, the NSA investigators have all gone through an intensive, multidisciplinary training course where they are taught interviewing techniques, report writing, how to track down sources of information and, particularly important, they are introduced to the full range of security disciplines: counterintelligence, physical security, industrial security, and clearance adjudications. Later in their careers they move into these other security disciplines and they continue to receive professional training. For example, all the clearance adjudicators attend the DCI Security Committee's adjudicators' course; the polygraphers are graduates of Army, CIA or other accredited basic polygraph courses (and internal advanced courses).

One further point on the applicant selection cycle. The NSA Office of Security has the advantage of full control, management and centralization of the security processes. The investigators, polygraphers, adjudicators, and security indoctrination personnel all work for the Director of Security who together with the heads of the personnel and medical services, report to the same NSA Deputy Director. Resources are conserved and a logical order of processing is possible. While a good case can be made for the reverse, NSA finds it best to conduct the polygraph interview early on, as this is the point where a significant number of applicants provide disqualifying information.

Some details on personnel security programs related to the on-board, cleared affiliates:

* The Office of Security conducts an annual Security Week program featuring distinguished speakers, displays, and videos covering such themes as espionage and terrorism.

* NSA personnel going overseas or on a special assignment are briefed by the Office of Security on countermeasures/counterintelligence concerns in the specific area of assignment.

* Security posters, videos, special lectures, and personal counseling are continuous.

* All management, administrative and survey courses under NSA auspices include presentations on personnel security.

* Affiliates are subject to aperiodic polygraph (counterintelligence/loyalty questions only) interviews and regularly scheduled investigative updates (including the counterintelligence/loyalty polygraph).

* Professional security officers are assigned to the staffs of major NSA components to advise and assist Agency managers in security programs.

* The Office of Security maintains an excellent professional working relationship with the FBI and other counterintelligence organizations, concerning the foreign intelligence threat to NSA personnel, facilities, information and equipment. Threat analyses and special investigations are conducted as needed.

The Polygraph

During the past two years, the Congress has been especially interested in government use of the polygraph, particularly proposals by DoD to expand the use of this technique. NSA Office of Security representatives briefed staffers from various Congressional committees and testified at hearings. NSA considers the polygraph its most effective personnel security screening tool and has a substantial body of information showing this - information which has been provided to Congress. The bottom line is that there are numerous examples - at NSA and other government agencies - of how the polygraph examination detected or deflected espionage or other criminal activity and provided relevant information available no other way. Just a few of those NSA examples, all from the last several years:

* An applicant for NSA employment who was about to retire from military service reacted to polygraph examination questions about intending to commit espionage against the United States. The applicant then described several recent visits to the Soviet embassy to make arrangements to defect.

* A contractor employee requiring sensitive access reacted to several polygraph questions relating to espionage. He then admitted that during two periods when he lived abroad he had been a scientific advisor to the Chief of a foreign military intelligence service, and that he might in the future pass classified U.S. information to that service. On his application forms he had concealed this activity, accounting for time abroad as being in an academic affiliation.

* Another contractor employee seeking NSA access reacted to polygraph questions on espionage. She then described in

detail the longtime espionage activities by her former husband on behalf of a foreign power.

* Other applicants for employment or contractor access have admitted to such crimes as murder, arson, rape, train-wrecking - admissions gained after the examiner detected reaction to relevant test questions.

The following documents contain detailed information on the value of the polygraph.

* Statement of Philip T. Pease, Director of Security, National Security Agency before the Armed Services Committee of the U.S. House of Representatives, 6 September 1984.

* The Accuracy and Utility of Polygraph Testing, 1984. Prepared by Norman Ansley, Chief, Polygraph Division, NSA for Deputy Under Secretary of Defense Stilwell.

* Polygraph Utility Study, February 1984 (an intelligence community study prepared for Congressional hearings -- not for release to the public).

In addition, the new DoD polygraph directive and regulation were issued on 24 December 1984.

An Evaluation of Personnel Security Techniques and Procedures

NSA considers the polygraph interview as unquestionably the best single personnel security tool. The vast majority of information that leads to disqualification of NSA applicants for employment/contractor applicants comes from the polygraph interview. Only NSA and CIA use the polygraph extensively for personnel security screening purposes. Recipients of NSA (and CIA) sensitive information at the State Department, the military services, Justice, and the NSC, among others, are not polygraphed. Also there is no large scale polygraph program in government for those who handle cryptographic keying and logic material. Our most secret electrical communications could conceivably be compromised through insider espionage - delivery of cryptographic key and related security information to the opposition. While it is unquestionably true that source and method information are concentrated at NSA and CIA, espionage by recipients of intelligence product can, and has, led to compromise of those sources and methods.

Other personnel security techniques and procedures are also extremely valuable, or could be. The periodic or aperiodic reinvestigation of on-board personnel - those with access to the secrets (as opposed to applicants) - needs increased attention. So does what we call security supervision. Some of our procedures in these areas are mentioned in an earlier section of this paper. A weak link in all personnel security investigations are the checks of police and FBI records, that latter being the centerpiece of the National Agency Check (NAC). Many police departments, in accordance with state laws, deny NSA (and the Defense Investigative Service) investigators access to their records. This is an incredible situation. Also, the NAC has been weakened because the FBI is overburdened in reviewing their records and their records are incomplete: we can no longer be sure that state and local police are reporting complete arrest records to the FBI. In those types of personnel security investigations which are currently limited to police checks and the NAC, an interview of the subject by a trained investigator would be a useful addition. Personal interviews of the individual are an excellent source of information but these interviews have to be done by well-trained people who know the personnel security and counterintelligence business as well as interview techniques.

The scope of investigative coverage needs to be upgraded, especially for SECRET access and for continued security assurance of personnel already holding access. This is resource intensive. The DoD group that studied the Harper case and security in industry has made a number of important recommendations in this area.

NSA's experience in industrial security may be of interest. We emphasize a partnership with the contractor special security officers (C/SSOs). We visit most of our Sensitive Compartmented

Information (SCI) contract facilities three times a year on a scheduled basis and at other times as needed. We conduct physical security inspections during the visits, but our emphasis is on a comprehensive program. During a visit our security officer may deal with physical and technical security matters, personnel security, security awareness briefings, and counterintelligence (such as meeting with FBI personnel responsible for counterintelligence in the particular area). These visits, however, are only a small part of the total program. We continually work with the NSA elements that the contractor is supporting. We require the company to dedicate a security officer to certain large projects and we look to that person as our on-the-scene agent. We try to avoid an adversarial, bureaucratic or check-list approach when dealing with industry. But our standards are high - we polygraph all of our contractor affiliates as a condition of initial access and they are subject to counterintelligence scope polygraph examinations thereafter -aperiodically or as part of a scheduled investigative update.

In conclusion, I want to commend for the record the people who work for me in the NSA Office of Security. They are a highly skilled, dedicated and well-trained group of men and women dealing with sensitive and difficult matters. We believe we have an excellent personnel security program. We hand pick people for the Office of Security. They in turn apply that same sense of individual attention to each investigation and polygraph examination, to the processing and clearance adjudication of each case, to the continuing security education, counselling and security assurance of our cleared workforce and to the rights of the individual.

STATEMENT FOR THE RECORD

SUBMITTED BY

THE

UNITED STATES NUCLEAR REGULATORY COMMISSION

TO THE

SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

FOR THE HEARING ON
THE GOVERNMENT'S PERSONNEL SECURITY SYSTEM

SUBMITTED: FEBRUARY 1985

Introduction

It is the policy of the Nuclear Regulatory Commission (NRC) to carry out its responsibility for the security of the nuclear energy program in a manner consistent with traditional American concepts of justice. To this end, the Commission established the NRC's Personnel Security Program, required by the Atomic Energy Act (AEA) of 1954, as amended, and implemented by Title 10, Chapter I, Code of Federal Regulations--Energy (10 CFR) Part 10, "Criteria and Procedures for Determining Eligibility for Access to Restricted Data or National Security Information or an Employment Clearance" (Enclosure 1). The NRC Personnel Security Program serves a threefold purpose: (1) to determine the character, associations, and loyalty of NRC employees, contractor employees, licensee employees, and others who require access to classified information, or sensitive unclassified information; (2) to assure that persons employed by the Federal Government are reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the U.S., consistent with the provisions of Executive Order 10450, "Security Requirements for Government Employment"; and (3) to comply with the special security requirements of other Government agencies, such as the Central Intelligence Agency (CIA) which permit our employees to interact with these federal agencies on classified matters, when necessary. The NRC Personnel Security Program is centrally administered and directed by the Director of Security.

By authority of Section 161 d., AEA, the NRC is excepted from the competitive Civil Service and the Classification Act of 1949. All appointments to NRC are made after suitability for employment evaluations based on the standards in NRC Manual Chapter 4108, Appendix Part III, "Merit Selection" (Enclosure 2). In addition, Section 145 b., AEA, specifically requires that every NRC employee must be found eligible for and granted an access authorization (security clearance) as a condition of employment.

In December 1982, the NRC reevaluated its Personnel Security Program, and revised the criteria used for determining the sensitivity of NRC employee and consultant positions and the corresponding background investigation and level of security clearance which they required. This reevaluation resulted in reducing the number of full field background investigations (BI) from 2,962 to 1,821. These position sensitivity criteria and corresponding investigative and clearance requirements are set forth in NRC Manual Chapter 2101, Appendix Part VI "Personnel Security Program," paragraph B (Enclosure 3).

Today, 12 of NRC's 3,817 positions are designated as of a high degree of importance or sensitivity under Section 145 f., AEA, requiring an FBI BI. Additionally, approximately 1,821 NRC positions are designated critical-sensitive requiring an OPM BI and 1,984 positions are noncritical-sensitive requiring an OPM National Agency Check and Inquiry (NACI) investigation. NRC has no nonsensitive positions. Of the 1,833 positions designated as of a high degree of importance or sensitivity, or critical-sensitive, 40 are the NRC equivalent to OPM's Special Sensitive designation requiring access to Sensitive Compartmented

Information. NRC has approximately 50 critical-sensitive automatic data processing (ADP) positions, equivalent to ADP-1. The remainder of NRC's ADP positions are designated as noncritical-sensitive, equivalent to ADP-II. In addition to its employees and consultants, NRC has an estimated 6,000 active security clearances granted to other personnel. Approximately 5,000 are NRC licensee employees and 1,000 are NRC contractors or employees of other Government agencies who require or who may have access to NRC classified information.

NRC power reactor licensees have their own personnel security system. The American National Standards Institute (ANSI) has developed a security standard, ANSI Standard 3.3, "Security for Nuclear Power Plants" (Enclosure 4), which has been adopted by most nuclear power plant site operators. This standard provides for in-depth preemployment screening of plant employees, psychological evaluation, and a continuing behavior observation program. ANSI Standard 3.3, however, does not pertain to the Government's security clearance program for access to classified information. The standard augments the NRC regulatory program and is intended to provide additional assurance that acts of sabotage are not committed against nuclear plants that could endanger the health and safety of the public.

Access

As indicated, each NRC employee must possess an NRC security clearance as a condition of employment whether or not access to classified information is required. The level of clearance necessary is based on the position sensitivity criteria. The NRC grants two levels of security clearance: "Q" and "L." A "Q" security clearance permits access on a need-to-know basis up to and including Top Secret National Security Information (NSI) and Restricted Data (RD). An "L" security clearance permits access on a need-to-know basis up to and including Secret NSI and Confidential RD. See Enclosure 5 for a listing of NRC security clearance grants and terminations up to December 1, 1984.

Currently, 124 (.03%) NRC employees are authorized access on a need-to-know basis to Top Secret information. Approximately 2,520 (66%) NRC employees have ongoing or frequent access to Secret and/or Confidential information. The remaining one-third may have occasional or infrequent access.

The NRC's criterion used to determine who may have access to classified information or to facilities of other Government agencies or their contractors involved in classified work (e.g., in the course of a classified visit) is twofold, i.e., does the individual have a need-to-know and does he/she possess the level of clearance necessary for the type and classification level of information at the facility? The "need-to-know" is normally determined by the individual's supervisor and the custodian of the information. His/her level of clearance is certified/verified by the NRC Director of Security, who is responsible for the overall NRC Personnel Security Program.

Background Investigation

The AEA specifies that personnel security investigations for NRC be conducted either by the FBI or OPM. NRC may, however, accept an investigation and report on the character, associations, and loyalty of an individual made by another Government agency if the report was used to grant a security clearance, providing the scope and extent of the investigation meet the NRC's standards.

NRC uses four basic types of investigations: a full field or Background Investigation (BI), a National Agency Check and Inquiry (NACI), the National Agency Check (NAC) and the Periodic Reinvestigation (PRI). The scope of each investigation is detailed on Enclosure 6.

NRC employees occupying positions designated as of a high degree of importance or sensitivity, or critical-sensitive, require a "Q" security clearance based on a BI. NRC employees occupying noncritical-sensitive positions require an "L" security clearance based on an NACI.

Contractor and licensee employees requiring a "Q" security clearance for access to Secret or Top Secret RD, or Top Secret NSI are subject to an OPM BI. Those requiring an "L" security clearance for access to Confidential RD or Secret NSI are subject to an NAC. Currently, no licensee employee has a "Q" clearance.

NRC generally requests four types of investigative services from OPM: (1) 120 day "turnaround" service for BI's costing $1,375 per BI, (2) 35 day expedite service for BI's costing $1,825 per BI, (3) 75 day service for NACI's, and (4) 60 day service for NAC's. NACI's are done at no cost for Government employees whereas NAC's cost $8. While NACI and NAC turnaround time has remained relatively constant, turnaround times for BI's have lengthened during the past 2 years to: (1) 9 to 13 months for 120 day service and (2) 3 to 6 months for 35 day expedite service.

These investigative delays, which we understand are attributable to the shortage of OPM investigative and support staff, have had a very adverse impact on NRC's ability to utilize qualified personnel, especially in the scientific and technical disciplines essential to NRC's licensing and regulatory mission. This has resulted in less than fully productive use of many employees (e.g., resident inspectors, or individuals requiring access to classified information) until the completion of the required investigation and grant of security clearance. Resident inspectors serve as the clearest example of this situation since they are not permitted free access to the licensee's nuclear power reactor site until NRC certifies to the licensee that the required investigation as to the inspectors' honesty, trustworthiness, and reliability has been conducted and a "Q" security clearance granted to the inspector. NRC has been forced by these investigative delays to hire and employ personnel in critical- and noncritical-sensitive positions prior to the completion of the required investigation and grant of security clearance.

However, NRC has consequently had to implement administrative controls and security safeguards for filling positions prior to the completion of an investigation. Those applicable to NRC Headquarters and Regional Offices are set forth in NRC Manual Chapter 2101, Appendix Part VI, paragraph G. Approval authority for preappointment investigation waivers is limited to the NRC's Executive Director for Operations (EDO) based on a written request for use of this authority from the Directors/Deputy Directors of Headquarters Offices or from the Administrators/Deputy Administrators of Regional Offices.

All requests must specify the effect(s) on NRC operations or programs if the individual is not employed as soon as possible. Additionally, each request must state that administrative controls will be established to assure the individual will not have access to classified information until the required investigation is completed and a security clearance is granted. Prior to the request being sent to the EDO for approval, the applicant's SF 171, "Personal Qualifications Statement," personnel security forms, and the results of pre-employment checks are reviewed by the cognizant personnel office and Division of Security personnel to insure there is no information contained therein which reflects unfavorably on the applicant's suitability for employment or eligibility for security clearance. A request to OPM to initiate the required investigation is made simultaneously.

NRC has found that the scope of the OPM BI and the scope of the NACI are adequate. Additionally, OPM has various scopes/options of investigation coverage available which permit NRC a great deal of flexibility to concentrate or expand on certain areas (e.g., alcohol/drug abuse) should the need arise. NRC prefers and receives the full narrative report from the OPM and the FBI as opposed to the summary or report by exception format. The narrative style provides the adjudicator with an in-depth description of the individual on which to base a security decision.

Adjudication and Due Process

An NRC applicant's basic suitability for employment is initially determined by the cognizant NRC personnel office in accordance with the standards and requirements set out in NRC Manual Chapter 4108, Appendix Part III. If an applicant is initially found suitable for employment, the required security investigation is initiated and, upon completion, reviewed and adjudicated by the Division of Security.

Investigations are centrally adjudicated by Division of Security personnel in accordance with the standards and requirements set out in 10 CFR Part 10. All clear (no adverse information) investigations result in security approval and notification to the cognizant personnel office of security clearance grant. If the investigation contains adverse information of a suitability nature that, had it been known or admitted earlier, might have precluded an individual from being found suitable for employment, the investigative results are coordinated with our legal staff and with senior personnel officials. Removal action, if warranted, is then initiated. To date, an estimated 15 individuals have been removed during their probationary employment period based on suitability information provided by personnel security investigations. If the individual is found suitable for NRC employment, the adverse information is then reviewed by the NRC Division of Security, Facilities and Personnel Security Branch, in accordance with 10 CFR Part 10.

The NRC's personnel security review and adjudication system and procedures have been established to ensure fairness, impartiality, and thoroughness in accordance with the standards and criteria of 10 CFR Part 10. NRC's personnel security analysts and senior adjudicators are security professionals who have demonstrated mature judgment, sound common sense, and skill in the interpretation and application of the criteria in 10 CFR Part 10. These individuals have a thorough knowledge of pertinent statutes, directives and regulations. They are also familiar with investigative and law enforcement practices and procedures.

Training of persons involved in the security adjudication process includes on-the-job training and attendance at various courses offered by other Government agencies, such as "Adjudication for Sensitive Compartmented Information Access" sponsored by the CIA, and "Suitability and Security Adjudication" sponsored by the OPM. On-the-job training embraces review of statutes, directives, discussions with and instructions from senior officials, participation in complex case analysis, and security interviews with applicants for security clearance under the personal direction of the Branch Chief or other senior adjudicators. As a precautionary check, the senior adjudicator is responsible for evaluating the adjudicative actions of the other personnel. Likewise, the Branch Chief evaluates the senior adjudicator.

Our analysts and adjudicators are also provided general adjudication guidelines to complement on-the-job training and course attendance. These guidelines are incorporated into the Branch's Standard Operating Procedures and are updated and revised as required.

We require a written analysis of all cases containing information believed by the analyst/adjudicator to be adverse under the criteria in 10 CFR Part 10. We require the analyst/adjudicator to clearly show that all information, favorable and unfavorable, adverse and mitigating, has been considered and evaluated in terms of its relevance, recency, and seriousness. The analysis must conclude with a recommendation to grant security clearance, if warranted, or for such additional action as may be necessary to resolve the issues of concern, such as interview, additional investigation, and psychiatric evaluation, in accordance with Subparts B and C of 10 CFR Part 10. All NRC adverse case analyses and recommended actions are reviewed by the senior adjudicator and/or the Branch Chief prior to any action and, if deemed necessary, are also coordinated with our legal staff. All cases which cannot be favorably resolved by the Branch Chief are referred to the NRC Director of Security, with a recommendation for administrative review under Subpart C of 10 CFR Part 10.

When information is received which raises a question concerning the continued eligibility of an individual for a security or employment clearance, the NRC Director of Security, may recommend to the NRC EDO the suspension of security and/or employment clearance in accordance with the procedures in Subsection 10.21 of 10 CFR Part 10 pending a final determination of the individual's continued eligibility.

When information is received concerning alcohol/drug abuse by an NRC cleared employee, the policies and procedures of the NRC's Alcohol and Drug Abuse Program apply. These are set forth in NRC Manual Chapter 4161, Appendix Part

IV, "NRC Alcohol and Drug Abuse Program" (Enclosure 7). Rehabilitation under this program would normally mitigate any need to initiate review of the person's continued eligibility for NRC security/employment clearance under 10 CFR Part 10.

It is appropriate to note that all those involved in our adjudicative and administrative review process are very careful to avoid the identification of any source who has provided adverse information after he/she has been assured of confidentiality, i.e., the protection of source's identity. If the information is corroborated by other sources, it is usually not necessary to introduce the specific information provided by the confidential source into any security interview or hearing. However, if we believe that the specific information provided by the confidential source would be essential to the conduct of a hearing, we would recontact the source to request a release from the promise of confidentiality and determine whether the source would appear and testify at a hearing. The Conduct of Hearing procedures are specifically set out in Subsection 10.28 of 10 CFR Part 10. To date, neither the Privacy Act nor any other statute or ruling has required the NRC to reveal the confidential source of adverse information to applicants or employees.

During the past four fiscal years, NRC has not denied any applications for security/employment clearance, but has revoked one security/employment clearance under 5 USC 7532. It should also be noted, however, that approximately 12 individuals, about whom serious adverse information was known, voluntarily withdrew their applications for employment/security clearance prior to the completion of the adjudicative and administrative review process. NRC's due process procedures for individuals whose initial or continued eligibility for security/ employment clearance is in question are contained in 10 CFR Part 10, Subpart C.

Periodic Reinvestigations

NRC's Reinvestigation Program is set forth in NRC Manual Chapter 2101, Appendix Part VI, paragraph O. One of the principal cost-effective revisions to the NRC Reinvestigation Program that resulted from NRC's 1982 comprehensive review of its Personnel Security Program was the adoption of the OPM Periodic Reinvestigation (PRI). The PRI, costing $75 a case, replaced the BI reinvestigation previously costing $1,375 a case. The PRI is conducted every five years on each NRC "Q" cleared employee and consultant, except NRC Commissioners and employees requiring access to SCI, who continue to be subject to the BI reinvestigation. In NRC's judgment, the PRI maintains the necessary reinvestigative coverage of these issues raised most often in BI reinvestigations relating to criminal activities, financial responsibility, mental illness, and alcohol and drug abuse at significantly less cost. Should a PRI disclose adverse information, expanded investigative coverage would be requested, if warranted.

The total annual cost for PRI's varies from year to year depending on the number of "Q" cleared employees whose prior investigations become five years old. Most recent reinvestigation costs and Fiscal Year (FY) 85 and FY 86 cost projections are in Enclosure 8.

NRC applies the same adjudicative standards in 10 CFR Part 10 to determine an employee's continued eligibility for security/employment clearance under the Reinvestigation Program as applied to determine initial eligibility. No adverse decisions have resulted from our Reinvestigation Program to date.

Related Information

The Office of Management and Budget has recently approved NRC's revised Part 2 of the Personnel Security Questionnaire (PSQ) (Enclosure 9). Several specific questions have been added to the PSQ which elicit from the applicant relevant information in the areas of financial responsibility, mental illness, and alcohol and drug abuse.

Through reciprocal security clearance agreements with the Department of Energy (DOE) and the Defense Industrial Security Clearance Office (DISCO), NRC may grant NRC "Q" or "L" security clearance to individuals of joint interest who hold a valid DOE or DISCO clearance based on a comparable investigation within the last five years. These agreements and implementing procedures eliminate the need for NRC to obtain and review existing investigations and enable us to rely on DOE/DISCO clearance decisions which are based on criteria and procedures comparable to NRC's. These security clearance certification agreements result in reduced security clearance processing times, administrative paperwork and forms completion burdens and in reduced costs for applicants, contractors, licensees, and the Government.

In addition to the Personnel Security Clearance Program outlined above to protect classified/sensitive unclassified information, NRC has developed a Material Access Authorization Program (MAAP) for the protection of Special Nuclear Material (10 CFR Part 11, Enclosure 10). The jobs requiring the two levels of access authorizations have been identified by all of the licensees and accepted by the NRC. Prior to implementation, minor revisions to the regulations are being pursued which significantly reduce the burden on both the licensees and the Government by allowing acceptance of existing federal clearances based on equivalent investigations. The MAAP specifies the OPM BI as the basis for grant of a "U" special nuclear material access authorization and the NAC as the basis for grant of an "R" special nuclear material access authorization.

The procedures and criteria in 10 CFR Part 10 are used in the MAAP adjudication process in accordance with the provision of Subsection 11.21 of 10 CFR Part 11.

3M STATEMENT TO THE

SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

UNITED STATES SENATE COMMITTEE ON GOVERNMENT AFFAIRS

"COMMENTS ON THE FEASIBILITY OF A SECURITY CONTROLLED COPYING SYSTEM"

MARCH 1985

Statement of:

P. J. Muldowney
Marketing Director
Safety & Security Systems Division/3M
St. Paul, Minnesota

J. E. Klinzing
Government Markets Manager
Office Systems Division/3M
St. Paul, Minnesota

3M Company welcomes this opportunity to respond to the request from the U.S. Senate Permanent Subcommittee on Investigations to participate in the subcommittee's study of the problems of protecting classified materials and information. Our contribution to this study will address the feasibility of protecting documents from being copied on an office copier and controlling the removal of classified documents from a designated environment.

By way of background, we would like to explain 3M's commitment to developing highly technical and sophisticated products for many markets.

3M is a worldwide, diversified manufacturing company with about 87,000 employees and business operations in about 50 countries. Our 40 operating divisions produce more than 50,000 products, with annual sales of more than $7 billion.

3M has a strong commitment to technological development, devoting 7.5 percent of sales to new product research and development. In fact, 25 percent of each year's sales come from products or services that were new in the previous five years. To foster opportunities for new product development, 3M has a "15 percent" rule, an informal policy of allowing technical researchers and scientists to spend as much as one day out of seven working on pet projects of their own.

The association between the United States Government Intelligence and Security Community and 3M Copiers goes back to 1949 when we developed the first totally dry copier, the 3M Thermo-Fax Machine. The Central Intelligence Agency, established only two years earlier under the National Security Act of 1947, visited our laboratory, in November 1949, for a demonstration of the Thermo-Fax. In February 1950, the Agency purchased 12 of the first 30 machines manufactured, along with 160,000 sheets of copy paper, and, in so doing, became our first customer for copying equipment.

Since our beginning as a manufacturer of copying equipment and supplies, a number of our latent image technologies have been employed to provide security measures in government activity. Such products as water soluble copy paper and heat sensitive copying systems, which can be developed with flat-irons, radiator heat or a match, are examples.

3M's commitment to developing new technologies in response to market demands led to the development of document security products more than 15 years ago, principally, the Tattle-Tape Detection System.

The Tattle-Tape System relies on a thin magnetic strip coated with a special metal alloy that is concealed in or attached to books, periodicals or documents. Some of the markers have a very aggressive adhesive, so that they can be inserted permanently along the spine of a book or attached to individual pages of a written document.

Any unauthorized removal of protected materials through exits that are protected by outporte detection panels sets off an audible or visual alarm. The outportes can be combined with locking gates, providing flexibility in controlling, channelling or restricting traffic flow, as required. This detection system is being used to protect documents in U.S. intelligence and defense contractor applications.

One of our current copiers accommodates another security function, which is a topic of this committee's study, polygraph tests. The 3M Continuous Copier can be used for copying polygraph test results. It copies lengths up to 415 feet.

As the manufacturer of more than 50,000 products, the above are but a few 3M products which directly relate to special government needs for protecting information and our national security. They substantiate that we have been aware of the need for protecting classified information and materials.

It has been reported that the United States Government has in excess of 17,500,000 secrets, and, if they were stacked, their height would equal the height of eight Washington Monuments. It has also been stated that, since 1973, this country has had more espionage cases than it has seen in the last 30 years. The magnitude of the problem and the increase in incidents involving unauthorized copying of classified documents drew 3M's attention to the problem.

It is difficult not to be aware of threats to the national security posed by foreign intelligence gathering services, and the threat is growing. At an October 11, 1984, briefing, Vice Admiral Edward A. Burkhalter, Director, Intelligence Security Staff, Office of the Director of Central Intelligence, reported that there are 2,500 Soviet Bloc officials and 4,000 other foreign officials currently stationed in the United States, and that an estimated third of these people are intelligence officers.

Recently, there have been several highly publicized cases of espionage which have involved the transfer of classified information through providing copies of documents to foreign intelligence groups.

Probably, the most publicized case in the last 10 years is the Christopher Boyce and Daulton Lee crime of providing highly sensitive data to the Russian Embassy in Mexico City. They were arrested in 1977, after nearly two years of providing secrets to the Russians. The compromise of this information might never have started if a deterrent to making copies had been in place, and the removal of classified documents from the environment had been exhibited. These men were not trained spies, they were opportunists, as were most of the recent violators of our national security.

William H. Bell, formerly of Hughes Aircraft, passed radar and missile data to a Polish intelligence officer for $110,000. Both were captured in 1981. Bell had little difficulty getting documents from where he had worked.

James D. Harper, apprehended in 1983, received $250,000 from Polish intelligence services over an extended period of time. Volumes of information, including Minuteman data, was involved. One news article stated: "Harper allegedly obtained photocopies of some of the defense material through his late wife . . . a secretary-bookkeeper at Systems Control, Inc. . . ."

Richard W. Miller, FBI agent in Los Angeles, passed on Bureau information to the Soviet KGB.

In the same news story, in October 1984, two other incidents were revealed as having taken place about the same time. Samuel Morison, of the Naval Intelligence Support Center, gave away classified photos, and an Army sergeant double-agent gave classified information to an East German woman. (The woman was charged with receiving classified information.)

Thomas Cavanaugh attempted to pass on Northrup Advance Systems Division's U.S. Stealth Bomber secrets to the Soviet Union. The FBI intercepted his efforts, and arrested him. Cavanaugh pleaded guilty March 14, 1985.

The preceding are some of the more recent security violations that have been uncovered. It is alarming to speculate about other surreptitious events that have not been identified, or may just be getting started.

The office copying machine provides an easy method for making unauthorized copies of classified information. In the government and government related projects, copying of secure information is a very large and very real problem. Research for a viable solution to this problem has probably been going on ever since copiers became available. To date, security measures to control the problem include: establishing policy, limiting access to sensitive information; maintaining log books, key or card access to machines; guarded environments, operator attended equipment, and the two-person rule requiring two people to make a copy. There are probably other precautions to take, but the problem still exists today.

3M first began pursuing a solution to the security problem in the late 1970s, as the result of an inquiry from the Federal Government. Then, as throughout our efforts on the subject, market information was very difficult to obtain, due to the nature of the subject of security. There definitely is no single source for information, such as market potential, product requirements, value of the application, what added costs are acceptable for protecting secrets (what is the value of a secret?). (In William Bell's case, the Poles and the Soviets saved hundreds of millions of dollars in research and development alone.)

Realizing there was no road map available, we proceeded to investigate the various avenues of concern by studying the market and interviewing government and prime contractor people to gain some insight on security and its requirements. At this same time, some spare time thinking began in our laboratory.

Though many of the critical questions are still unanswered, in 1982 some product development effort began, based on the size of the market and extent of the problem which existed. After sorting through the variety of comments gathered from the field, a product description was written to meet the most often heard objective that our potential customers cited, which was: "To stop the casual offenders who violated security regulations because there are no effective deterrents. We are tired of seeing our classified information in the newspaper."

In January 1983, a feasibility product was demonstrated and, in March, a patent application was filed. During early 1983, private showings were made to selected government and industry people. Customer impressions were favorable and encouraging, but it rapidly became apparent that "casual offenders" were not the only target. As a result, enhancements were made to the product to tighten security on the machine and improve the supply item.

During January 1984, five prototype machines were developed containing several improvements recommended by our contacts. Quality assurance testing was conducted for two months, and the copiers were prepared for field test.

During the summer of 1984, tests were conducted in three locations, and a demonstration system was installed in 3M's Washington office for private presentations. The results of these activities overall were positive, with more constructive ideas coming forth.

Upon completion of this test phase, the products were returned to St. Paul for final refinement, and additional features have been added. In our opinion, feasibility has been confirmed.

To verify our opinion, two final versions of our prototype security controlled copier systems are currently being tested in government and industry.

3M technologies incorporated in the system come from a number of 3M divisions. These, and other capabilities of the company, are leading to potential solutions for other information security problems which exist in the marketplace.

A general description of the system is as follows:

The security option for the Model 787 copying machine is a feature added to the machine which will allow the machine to detect the security classification of an original to be copied. If the machine senses that a document is classified, there will be no copy produced, and alarms are sounded to alert the proper authorities of an attempt to copy classified material.

Documents are classified by attaching a small security label to the document via a very aggressive adhesive. Any attempt to remove the strip will leave physical evidence of tampering.

There are two modes of operation for the machine: normal and bypass. The modes are controlled by a key switch. One key will turn left, which puts the machine in the bypass mode. The other key turns right to reset the machine after an alarm occurs.

In the normal mode of operation, the document loader cover is latched down and the machine will only operate when an original is put into the document loader entrance. In this mode, the machine exit area, the transport drawer, the top cover and the secondary paper feeder are locked. In this mode, if an original is not classified, the machine will operate as a normal 787 machine - except the maximum original size is 8 1/2 x 11 inches. If the document is classified, the machine senses the strip, inhibits the copying process and an alarm is activated. Remote alarm outputs are available on the rear of the machine. When an alarm occurs, the original is retained in the document loader, and a blank copy exits the machine. An alarm condition can only be cleared by an authorized person with a security key.

In the bypass mode of operation, the machine can make copies of classified documents. The document loader is unlatched electronically, as is the secondary paper feeder. This gives the authorized operator access to the stock of pre-labelled paper which is normally secured in the secondary paper feeder. This also allows the operator to make book copies or copies of 14 inch originals. When in the bypass mode, the alarms are sounded continuously to alert the area that classified materials are being copied.

To complete the system, there is a need to control ingress and egress of the facility containing classified information and the security copier. The 3M Tattle-Tape outporte detection panels offer the highest level of security protection against unauthorized removal because they can detect the special security labels through clothing, purses, briefcases and layers of other documents. In fact, the Tattle-Tape Detection System is being used to protect documents in U.S. intelligence and defense contractor applications.

3M introduced the Tattle-Tape Detection Systems in 1969, and they are now used by thousands of libraries and bookstores. These systems have been proven to reduce book losses by an average of 85.5 percent. The same technology is used to reduce shoplifting in retail stores.

Of course, 3M is not the only company marketing detection systems for libraries and retail stores; 3M is a major player in a highly competitive market. However, history makes it clear that successful business strategies are based on conditions within an industry, anticipating those conditions and developing products to meet them.

It is on this basis that 3M wedded two technologies in which we had a strong market presence: detection products and office copying machines to develop a security controlled copier system.

STRENGTHS OF SYSTEM

A. Serves as normal office copier for standard copying requirements.

B. Human factors considerations for security copier.

C. Modular construction applicable for servicing in a security environment.

D. Prevents unauthorized copying of classified materials when special security label is applied.

E. Prevents removal of documents from a secured area.

F. Prevents substitution or tampering with originals in the process of being copied.

G. Provides audible and visible enunciation to security personnel.

H. Has optional provisions for surveillance cameras, both of video and photographic types.

I. Security label will offer protection for books, training manuals and other large items.

J. Has provision to allow copying of classified materials by authorized personnel, using bypass key.

K. Security system can be configured in a flexible manner, either as a copier or a complete system with optional features.

To our knowledge, no viable competitive system has been developed. We are aware of competitive activity on the matter, but nothing which has been considered a successful solution. Two companies are working with devices which provide a monitoring record of copies made while identifying the user by personal identification number. Another company sells an uncopyable burgundy paper. A couple of companies have announced systems, but we have not heard of them for a couple of years.

At this point, we do not have the panacea. It is difficult to imagine that it will ever be accomplished. The professional spies have a variety of devices at their disposal. What we do have is the best deterrent available to prevent the proliferation of unauthorized copies and their removal from a controlled environment. We also have a technology which is directly and economically adaptable to provide protection on facsimile and teletype equipment, as well as other types of office equipment.

The 3M copier, the Model 787, used to develop the concept is a remanufactured product which has performed very reliably in the market as a copier. The 787 also contains human factors for adaptation to a security copier.

One test location evaluator stated in his report: "With respect to the hardware, this site experienced no problems with the security hardware installed on the 3M copier. After initial set-up and adjustments were made, the additional security devices performed commendably. In a closed environment, the 3M secure copying system, as is, would be beneficial to a small project just starting out."

Today's product has application in the market, but the future of the program rests with current and future equipment. The present technology is adaptable to these products which are feature rich and conform to the copying requirements of most functioning facilities. In addition, we have further system and supply development plans which provide even more capabilities for protecting classified information.

3M would like to contribute to solving the problem of protecting sensitive documents. However, the challenges of developing products for the security and intelligence community are identifying the market potential and gaining product acceptance without providing the "cure-all" for the problem immediately. 3M must decide whether to continue funding research and development activities for products under the existing circumstances.

We sincerely appreciate this opportunity to share our efforts with this subcommittee, and are available for any additional information that may be required.

4/2/85
JK3p

EXHIBIT NO. 1

A REPORT TO THE DEPUTY UNDERSECRETARY OF DEFENSE FOR POLICY

ANALYSIS OF THE EFFECTIVENESS OF THE DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY PROGRAM AND RECOMMENDATIONS FOR PROGRAM IMPROVEMENT

DEPARTMENT OF DEFENSE
INDUSTRIAL SECURITY REVIEW COMMITTEE

DECEMBER 10, 1984

ABBREVIATED VERSION

PREPARED FOR DISTRIBUTION AT HEARINGS OF THE
U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
"U. S. GOVERNMENT PERSONNEL SECURITY PROGRAM"
APRIL 1985

COMMITTEE MEMBERS

Daniel R. Foley, Co-Chairman
Deputy Assistant Inspector General, DoD
Criminal Investigations Oversight

John R. Hancock, Co-Chairman
Chief, Programs Management Division
Defense Investigative Service

Kathleen A. Buck
Assistant General Counsel (Legal Counsel), DoD

John E. Frields
Principal Assistant, Industrial Security
Office of the Director, Security Plans and Programs
Office of the Deputy Under Secretary of Defense for Policy

Alfred W. Hazen
Northwestern Regional Director
Defense Investigative Service

Alvin L. Madison
Program Director, General Intelligence
Office of the Assistant Inspector General for Auditing, DoD

INDUSTRY ADVISOR

Jerry M. Dolan
Director of Corporate Security and
Administrative Services, Aerojet General Corporation

REPORT OF THE DOD INDUSTRIAL SECURITY REVIEW COMMITTEE

EXECUTIVE SUMMARY

As a result of the arrest of James Durward Harper, Jr., for alleged espionage activity involving a Department of Defense (DoD) contractor facility, the DoD Industrial Security Review Committee was formed to "analyze the effectiveness of current industrial security requirements and develop recommendations for program improvement."

After a comprehensive study of the Defense Industrial Security Program (DISP), the Committee has completed its work and offers this summary of principal findings, conclusions and recommendations.

It is important to note at the outset that the Committee did not consider it a part of its mission to evaluate the performance or quality of service provided by the Defense Investigative Service (DIS), which is charged with administering and overseeing the DISP. Rather, it was to evaluate the overall system of security within defense industry with particular emphasis on identifying various methods of strengthening the program and formulating specific recommendations for improvement.

The defense industry is immense in size and scope. The DoD engaged in 14.7 million contractual procurement actions in 1983 at a cost of $140.5 billion. It is recognized that each of these procurement actions did not involve a classified contract, but a significant portion did involve sensitive, leading-edge defense technology which requires security protection. Furthermore, considering the primary mission of the Department, which is to defend the security and national interests of the United States, lax security in sensitive defense production presents awesome consequences. To perform its mission, the Department must maintain in peacetime an ample and secure industrial base to facilitate the preparation and successful conduct of military operations. A fundamental concept, therefore, which guided the Committee in its study, was the belief that industrial security policy and procedures must ensure the proper protection of classified information in industry in consonance with national policies and goals and not unduly encumber defense production.

Currently, there are nearly 14,000 cleared defense facilities, over 1 million cleared contractor employees and approximately 16 million classified documents entrusted to their safekeeping. To oversee the DISP, the DIS has less than 200 industrial security representatives (inspectors) in the field, a small number in comparison to the size and complexity of the cleared defense industrial establishment.

Committee Recommendations

POLICY

1. Increase emphasis on counterintelligence and human reliability factors in the administration of the Defense Industrial Security Program in order to provide enhanced protection against unauthorized disclosure of classified material.

2. Prioritize defense contracts according to the cognizant procurement activities assessed sensitivity of technology and apply commensurate DIS industrial security resources.

3. Where feasible, promulgate general security policy to replace much of the inordinate detail contained in the current

Industrial Security Manual (DoD 5220.22-M). Furthermore, tailor specific security requirements for individual contractor facilities into contractors' Standard Practice Procedures (Security Manual), taking into account the local hostile intelligence threat.

4. Establish a special group of DIS industrial security representatives to inspect special access programs and related "carve-out" contracts. To the extent practicable, program managers should be encouraged to relinquish inspection responsibility of such programs to the DIS. Furthermore, the Inspector General, DoD, during audits of special access programs, shall determine that each program has been properly established pursuant to Executive Order 12356, and the DoD implementation thereof, and assess reasonable adherence with DoD contracting practices, contractor performance and management of program funds.

5. Strengthen the personnel adjudication process through establishment of adjudicative standards as opposed to adjudicative guidelines which shall be uniformly applied throughout the DoD.

6. Duplicative reviews in the Industrial Security Adjudicative process should be eliminated, any potential conflict of interest be removed, and a centralized DoD clearance organization be established. Also, obtain subpoena power to compel attendance of witnesses and production of records at the hearings in the Industrial Personnel Security Clearance Program.

7. Amend the current inspection schedule prescribed in the "Industrial Security Regulation" to take more effectively into account the volume and complexity of the classified activity at a particular DoD contractor facility. Discontinue routine inspections of "dormant" contractor facilities and

eliminate or significantly curtail inspections of "access elsewhere" facilities.

8. Require all contractor employees to report to the facility security department all instances of foreign travel for review by DIS representatives during the inspection effort.

ADMINISTRATION/OPERATIONS

9. The DIS establish a pilot program in which the industrial security representatives' duties as advisors to industry and regulatory inspectors are separate and distinct.

10. The DIS establish, publicize and administer a national DoD Industrial Security Hotline.

11. The DIS establish a pilot program, in coordination with industry and the military departments, for the assignment of industrial security representatives on a full-time or substantially full-time basis at extremely complex or particularly sensitive contractor facilities.

12. Alter the DoD security inspection rating system to provide for ratings of "superior," "satisfactory," "marginal" and "unsatisfactory" in order to provide a more meaningful evaluation of a contractor's system for safekeeping classified information.

13. The DIS provide a formal certification/accreditation training program for contractor industrial security personnel. The training program shall not be a mandatory requirement, however, the benefits of industry participation seem obvious, particularly smaller firms newly engaging in DoD classified contracts.

14. At the earliest practical time, DoD criminal investigative organizations should notify the DIS of criminal investigations indicating criminal conduct by cleared DoD contractors and contractor personnel.

LEGISLATION/REGULATION

15. Review current espionage laws that pose obstacles to the prosecution of individuals for the unauthorized disclosure of classified information.

16. Seek legislation limiting judicial and administrative review of DoD personnel security adjudications to the adjudicative procedures themselves and exclude the review of the adjudicative decisions of the Directorate of Industrial Security Clearance Review.

17. Amend the "Federal Acquisition Regulations" (FAR) or issue DoD implementing guidance to provide the authority to suspend and debar DoD contractors for serious security infractions.

PERSONNEL SECURITY

18. Negotiate the deletion of neighborhood and education interviews from the minimum investigative standards for a Special Background Investigation (SBI) mandated by Director of Central Intelligence Directive (DCID) No. 1/14. In addition, include subject interviews to the foregoing DCID as a mandatory investigative element of the SBI.

19. Enhance personnel security investigative standards and reduce the number and level of industrial clearances as follows.

a. Reprioritize the current system of selecting industrial personnel for periodic reinvestigation consideration. The present method of selecting personnel with the most dated investigations should be set aside in favor of a system which places priority on personnel who enjoy continuous or frequent recurring access to Top Secret, highly sensitive, or Sensitive Compartmented information.

b. Facility or personnel security clearances under the DISP should not be processed for defense contractors who provide services at sensitive facilities where access to classified information is not required.

c. DoD policy should be changed to permit the DIS cognizant security office authority to approve contractor employees for one-time or occasional access to classified information at a level higher than the personnel security clearance in effect. If recurring access is anticipated, approval would include initiation of the appropriate investigation.

d. Documentation for company granted Confidential personnel security clearance should be furnished to the DIS to be reviewed and recorded. In addition, such clearances shall be subject to automatic expiration 5 years from the date of issuance if justification for continued access is not provided. If justified, the clearance should be reissued by DIS following completion of a favorable national agency check.

e. DoD policy should be changed to permit use of the interim clearance investigative standards and criteria presently provided for by the "Industrial Security Regulation" (DoD 5220.22-R) for all collateral personnel security clearance requests received for processing.

f. All Top Secret and Secret industrial personnel security clearances should be subject to automatic downgrade to the next lower level of clearance if justification to retain the higher level clearance is not received by the DIS within 5 years from the date of issuance.

g. A local agency check (LAC), employment check, and credit check should be added to the minimum investigative requirements for a Secret personnel security clearance. Furthermore, a national agency check, LAC, employment, and credit check should be repeated every 5 years.

h. All personnel security questionnaires submitted to the DIS for processing should be accompanied by a Clearance Justification Data Sheet. The data sheet should include certification by the employee applicant, immediate supervisor, and responsible management official that the applicant for clearance requires access to classified information, as well as a completed counterintelligence questionnaire.

20. Contractor Standard Practice Procedures should prescribe disciplinary action for employee security violations.

PHYSICAL SECURITY

21. An affirmative system of controls should be established over after-hours access and reproduction equipment at cleared facilities. While universal control requirements should not be mandated, the individual contractor, in consultation with the DIS, should establish an adequate system,

considering the particular circumstances of the facility, and incorporate the details into the Standard Practice Procedures.

INFORMATION SECURITY

22. The DoD Inspector General should schedule an audit of the Defense Technical Information Center to ascertain if internal controls are in place and working to preclude the unauthorized access and disclosure of its scientific and technical products and services. About 2,100 registered users are cleared for access to Secret and Confidential information on over 200 technical and scientific subjects ranging from aeronautics to space technology. Moreover, a military counterintelligence organization should conduct a hostile intelligence threat assessment of the Center.

23. The DIS conduct proactive efforts to oversee compliance with requirements pertaining to public disclosures regarding classified contracts and related brochures, promotional sales literature and reports to stockholders, as well as presentations at symposiums, conventions and so forth.

24. Increase emphasis on security classification management through training and oversight.

25. Strengthen procedures for prevention of "bootlegging" of classified material by establishment of a termination briefing and required execution of a form certifying that the executor possesses no classified material.

Committee Perspective

While adoption of some of the recommendations may appear costly and labor-intensive, some recommendations will result in savings in costs and labor. The thrust of the recommendations is focused at strengthening the DISP through concentration of DIS resources in the most vulnerable areas, revising some methods of operation, and eliminating activities of limited security value. A complete listing of all the Committee's recommendations is located at page 130.

STUDY METHODOLOGY

The report of the Defense Industrial Security Review Committee (the Committee) is presented in a single volume, supplemented by various appendixes, and is based on two distinct research approaches. The first consists of the collection and compilation of statistical data concerning the scope, magnitude, and operations of the Defense Industrial Security Program (DISP) and the DoD Personnel Security Program, the latter of which was largely limited to its application to industrial employees. These data are presented in several sections and appendixes of the report. They are based on replies to a Committee letter soliciting comments and recommendations on all aspects of the DISP and its administration by the Defense Investigative Service (DIS). The letter was sent to 350 large and small defense contractors as well as various Federal agencies. Furthermore, a comprehensive questionnaire was sent to all DIS job series 080 personnel and other personnel of DIS whose duties and responsibilities include substantial DISP involvement. Also included and subjected to Committee analysis were quantitative data compiled separately by the DIS and issued by that agency as Monthly Management Reviews. The results of these sources of data are reflected throughout the report in the various discussions, conclusions, and recommendations contained therein. An overview of the DISP is attached for information at Appendix I.

The second approach is generally qualitative in nature. It covers many elements which cannot be analyzed through statistical measurement. Statistical material is included, however, where available and pertinent. Aside from the DIS, substantial inputs were provided by cleared defense contractor facilities, by various industrial associations, by the Military Departments, by various other DoD components, by elements of the Office of the Secretary of Defense, and by other non-DoD

U.S. Government Departments and Agencies. The contractors and industrial associations drew heavily upon information voluntarily supplied by their professional industrial security staffs, employees, and general membership, respectively.

Material was drawn from responses to letters, personal interviews, the media and group discussion. The letters and forums served as means to solicit information on pertinent aspects of the DISP, the current administration of the DISP, any relevant criticism of the DISP, and suggestions and recommendations to improve the Program or its administration/implementation.

Study Chronology and Scope

In late October 1983, General Richard G. Stilwell, the Deputy Under Secretary of Defense for Policy, authorized the Director, DIS, to form a panel to examine events associated with the arrest of James Durward Harper, Jr., for alleged espionage activity. The panel was to study the *modus operandi* of Harper, Harper's wife, and the security conditions of the contractor facility from which the classified material was diverted (Systems Control Technology, Inc.). Within this context, the panel was to analyze the effectiveness of current industrial security requirements and develop recommendations for improvement.

The panel held its initial meeting in November 1983, to review the known facts of the Harper incident and to develop a general study methodology. However, in view of the policy implications and to assist the panel with its responsibilities, General Stilwell decided in early December to redesignate the panel as the DoD Industrial Security Review Committee and place it under his auspices (Appendix II).

As a related matter in November 1983, the Acting Secretary of the Air Force sent a memorandum (Appendix III) to the Secretary of Defense expressing concern regarding the Harper espionage case and suggested that the DoD Inspector General conduct an objective review of the Defense Industrial Security Program. The Secretary of Defense replied in a memorandum (Appendix IV) that the Committee had been formed to "...conduct a comprehensive evaluation of the effectiveness of the DISP...."

In late December 1983, the Committee solicited written comments and suggestions for program improvement from approximately 350 cleared defense contractors and from selected DoD and non-DoD organizations (Appendix V).

By the end of January the Committee had reviewed the administrative inquiry of Systems Control Technology, Inc. (SCT) conducted by the DIS (Appendix VI) and had completed a visit to the Silicon Valley area of California where SCT is located to gain insight into the special security and counterintelligence problems of locales with a concentration of firms engaged in high technology defense work. The visit included interviews with local DIS industrial security personnel and a meeting at the Stanford Research Institute's International Center in Palo Alto, California, to discuss pertinent issues with ranking management and security officials from 22 Silicon Valley contractor facilities.

In order to enhance the depth and scope of the ongoing review of the DISP, the Committee developed and distributed a comprehensive questionnaire to all DIS personnel with substantial industrial security duties and responsibilities. The questionnaire addressed all pertinent aspects of the DISP and its administration by the DIS. The Committee received 170 replies to the questionnaire, which proved most valuable in the formation of initial issues and concerns warranting further analysis. A copy of the questionnaire, along with the compilation of the 170 responses received, is at Appendix VII.

The Committee made a number of visits to various Government activities to gather additional information deemed essential to a thorough examination of the relative strengths and weaknesses of the DISP. Accordingly, the Committee interviewed key officials during its travels to the Air Force Office of Security Police and the Air Force Systems Command (Contract Management Division), Albuquerque, New Mexico; U.S. Army Ballistic Missile Division, Huntsville, Alabama; Defense Technical Information Center, Alexandria, Virginia; Defense Industrial Security Clearance Office, Columbus, Ohio; Directorate, Defense Industrial Security Clearance Review, Office of the General Counsel, DoD, Arlington, Virginia; Department of Energy, Germantown, Maryland; National Security Agency, Fort George Meade, Maryland; Central Intelligence Agency, Tysons Corner, Virginia; the Federal Bureau of Investigation, Washington, DC; and DIS Headquarters. The Committee also attended and participated in the annual Security Committee meeting of the Aerospace Industries Association (AIA) in Tucson, Arizona. The Committee discussed many of its preliminary issues with the AIA membership as well as the eight attending DIS Regional Directors of Industrial Security.

The Committee conducted personal interviews with representatives from each of the Military Department counterintelligence organizations (Army Military Intelligence, Naval Investigative Service and Air Force Office of Special Investigations). These interviews included discussion of preliminary Committee issues and a solicitation of comments and recommendations. Details of the Harper, Bell/Zacharski and Boyce espionage cases, which are summarized at Appendixes VIII, IX and X, were also carefully reviewed and discussed.

A composite of Committee interim findings and suggested program improvements were presented, in draft form, to counterintelligence and security staff officials of the Office of the Deputy Under Secretary of Defense for Policy for their review and comment. These interim findings were also mailed to the Security Committee and Security Sub-Committee membership of the AIA and the National Security Industrial Association, respectively, for their review and comment. The response to these efforts was most enlightening and the comments received resulted in some adjustments to the Committee's conclusions and recommendations. Appendix XII is a compilation of personnel contacted during the study.

SUMMARY OF THE COMMITTEE'S RECOMMENDATIONS REGARDING CHANGES IN THE DEFENSE INDUSTRIAL SECURITY PROGRAM

1. Increased Emphasis on Counterintelligence and Human Reliability Within the Defense Industrial Security Program (DISP)

The DIS administration and oversight of the DISP should include a balance of administrative inspections and attention, in partnership with industry, to the human reliability aspects of the program with emphasis on the hostile intelligence threat. This would necessitate a closer alignment of the DIS with the counterintelligence community and development of a viable threat awareness program.

2. Priority Emphasis on Security of Sensitive Contracts

DoD procurement activities, employing a reasonable apportionment system, should prioritize classified contracts according to assessed sensitivity. Commensurate DIS resources would be applied to these contracts based on the assessed sensitivity.

3. Revision of the Industrial Security Manual

Where feasible, promulgate general security policy to replace much of the inordinate detail in the current Industrial Security Manual (DoD 5220.22-M). In addition, large segments of the Industrial Security Manual that have limited applications should be extracted and put in supplement or handout form. Furthermore, tailor specific security requirements for individual contractor facilities into contractors' Standard Practice Procedures (Security Manual), taking into account the local hostile intelligence threat.

4. DIS Inspection of Special Access Programs

a. That the Department of Defense Inspector General, during audits of special access programs, determine the adequacy of, and compliance with, DoD contracting practices, contractor performance, management of program funds and other areas of special access programs and carve-out contracts.

b. That the Office of the Deputy Under Secretary of Defense for Policy continue to support the audit efforts of the Department of Defense Inspector General and coordinate with DoD components the program access authorizations required by audit personnel.

c. That the DIS establish a special group of inspectors for special access programs and related "carve-out" contracts and that DoD components relinquish to the DIS inspection of these programs and contracts when determined appropriate by the sponsoring component.

5. Strengthening the Adjudication Process

The Committee recommends that the term "guidelines" be revised to read "requirements" and be applied uniformly in all cases.

6. Centralization of the Adjudication Function Within the Department of Defense

That the Deputy Under Secretary of Defense for Policy determine whether the Adjudication Division of DISCO is in fact performing adjudicative functions within the purview of the Administrative Procedures Act. Each case should be reviewed carefully once, subject to the approval of the individual in charge of the centralized adjudication function. Furthermore, that a separate study be conducted to assess the merits of centralizing the adjudication function (separately and distinctly from any investigative organization) within the Department of Defense for adjudication of all security clearances to include cases under the DISP. Finally, obtain subpoena power to compel attendance of witnesses and production of records at the hearings in the Industrial Personnel Security Clearance Program.

7. Revising the Frequency of Industrial Security Inspections

That the current inspection schedule prescribed by paragraph 4-103a, "Industrial Security Regulation," be replaced by a system that more effectively considers the volume and complexity of classified activity. The new system should also include sufficient flexibility to enable local managers to adjust workload and concentrate effort where most needed. Furthermore, that routine inspections of "dormant" facilities be discontinued and that inspections of "access elsewhere" facilities be eliminated or significantly curtailed.

8. Reporting of All Foreign Travel by Contractor Personnel

All cleared employees be required to report to the facility security department all instances of foreign travel for review by DIS representatives during industrial security inspections.

9. Creation of Separate Advisor and Inspector Roles of DIS Representatives

DIS should adopt a pilot program in which individual industrial security representatives function either as advisors to industry or as regulatory inspectors.

10. Establishment of a National Industrial Security Hotline

Establish a 2-year pilot national DoD Industrial Security Hotline Program within the Defense Investigative Service and appropriately publicize it.

11. Assignment of DIS Personnel to Extremely Complex or Particularly Sensitive Contractor Facilities

The Director, Defense Investigative Service, should develop and initiate a pilot program in coordination with industry for the assignment of industrial security representatives on a full-time or substantially full-time basis at certain complex and particularly sensitive contractor facilities.

12. Establishment of a Graded Defense Industrial Security Program Inspection Rating System

The DoD security inspection rating system be changed to provide for ratings of "Superior," "Satisfactory," "Marginal," and "Unsatisfactory." Moreover, DoD contracting activities should maintain close liaison with the Defense Investigative Service before the award of classified contracts.

13. Specialized Training Program for Accrediting Contractor Security Personnel

The DIS provide a formal certification/accreditation training program for contractor industrial security personnel. The training program need not be mandatory.

14. Notification of the DIS of Criminal Investigations Involving Cleared DoD Contractors and Contractor Personnel

At the earliest practical time, DoD criminal investigative organizations should notify the DIS of criminal investigations that indicate criminal conduct on the part of cleared DoD contractors and contractor personnel.

15. Legislative Base for the Defense Industrial Security Program

Establish a working group to draft new legislation that would carefully address the problems of prosecution of espionage including the need to declassify the information involved in the prosecution.

16. Legislation to Limit Administrative and Judicial Review of DoD Personnel Adjudication to the Adjudicative Procedures Themselves

A panel should be formed to study legislative initiatives to limit administrative and judicial review of DoD personnel security adjudications to the adjudicative procedures and to exclude review of the adjudicative decisions of the Directorate of Industrial Security Clearance Review.

17. Authority to Suspend and Debar Contractors for Serious Security Infractions

The Committee recommends amending DoD FAR Supplement 9.470 to clearly identify security violations that may be used as the basis for suspension and debarment. The DIS should be required to provide notice to the cognizant DoD suspension/debarment authority of all significant security violations on the part of cleared contractors or tneir cleared employees.

18. Revised Scope of Personnel Security Investigations

That negotiations be initiated to amend the Director of Central Intelligence Directive No. 1/14, dated 1 September 1983, to require subject interviews as part of the minimum investigative standards for the SBI and that currently prescribed neighborhood and education check/verifications be deleted from said DCID as required elements of investigative coverage.

19. Enhancement of Personnel Security Investigative Standards and Reduction of Industrial Clearances

a. The Deputy Under Secretary of Defense for Policy should revise the current system used to determine priority consideration for the conduct of periodic reinvestigations (PRs). The new system should identify those Top Secret-cleared (and perhaps those with Sensitive Compartmented Information access) who have continuous or recurring access to Top Secret information and should subject only those individuals to the PR requirements. Those who have never had access to Top Secret or who rarely have such access should be eliminated from PR consideration or placed on a low priority listing, as appropriate.

b. Clarify the policy to ensure that contractor personnel determined eligible to be processed for a NAC under physical-access-only circumstances do not qualify and shall not be processed for a personnel security clearance under the Defense Industrial Security Program.

c. The cognizant security office should be authorized, upon receipt of appropriate justification, to approve contractor employees for one-time or occasional access to classified information at one level higher than the personnel security clearance in effect.

d. All company-granted Confidential personnel security clearance documentation should be furnished to the DISCO for review, recordation, and a DCII check.

e. All company-granted Confidential personnel security clearances should automatically expire 5 years from date of issuance unless the need is rejustified. To remain valid for a longer period, an updated PSQ, Clearance Justification Data Sheet and Counterintelligence Questionnaire shall be received by the DISCO for review before the scheduled expiration date. Reissuance by the DISCO, if otherwise appropriate, shall be based on a favorable National Agency Check and shall remain valid as long as the employee has a need for access and remains employed by the same contractor.

f. Industrial personnel security clearance policies and procedures must be changed to permit the use of interim clearance procedures prescribed by the "Industrial Security Regulation," DoD 5220.22-R; and remove the requirement for contracting officer or higher level approval, for all personnel security clearance requests.

g. All Top Secret and Secret industrial personnel security clearances shall be subject to automatic downgrade to the next lower level of clearance when DISCO does not receive justification to retain the higher level clearance within 5 years from the date of issuance.

h. All Secret industrial personnel security clearances should be based initially on a National Agency Check, local agency check, credit check and employment check which shall be repeated every 5 years thereafter.

i. All personnel security questionnaires submitted to the DISCO, regardless of level, should be accompanied by a Clearance Justification Data Sheet.

j. All personnel security questionnaires submitted to the DISCO, regardless of the level of clearance requested, shall be accompanied by a completed counterintelligence questionnaire.

20. Documentation in Standard Practice Procedures Relating to Disciplinary Action for Security Violations

That contractors be required to establish in their SPPs company policy on disciplinary action to be taken against employees involved in security violations when culpability is established. The DIS shall be limited to advising and assisting the contractor in its preparation of the policy if requested.

21. System of Controls Over After-Hours Access and Reproduction Equipment at Cleared Facilities

a. The DoD should adopt a policy requiring cleared Defense contractors to develop and effectuate procedures that ensure that all persons working or visiting the proximity of repositories or areas used to store classified material during nonworking hours are monitored by continuous or intermittent means capable of preventing or detecting physical presence, unauthorized access, and removal of classified material from the premises.

b. The DoD should adopt a policy requiring cleared contractors to develop and place into effect procedures that ensure that reproduction equipment is monitored by continuous or intermittent means to prevent or detect the unauthorized copying of classified material. The specific control procedures shall be developed in consultation with the DIS and incorporated with the individual facility's Standard Practices Procedure and be subject to DIS inspections.

22. Access to the Defense Technical Information Center Classified Data

a. That the Inspector General, Department of Defense, schedule an audit of the Defense Technical Information Center to ascertain whether internal controls exist to preclude the unauthorized disclosure of and access to its scientific and technical products and services. The scope of the audit shall encompass procuring activity justification for authorizing the broad areas of interest for access by contractors.

b. That the Deputy Under Secretary of Defense for Policy designate a Department of Defense counterintelligence component to evaluate any potential threat to the Center from hostile intelligence services. In this regard, the appropriate countermeasures should be taken to protect its personnel, products, services and data base from potential compromise.

23. Proactive Efforts by the DIS to Prevent Unauthorized Disclosures

The DIS should incorporate proactive efforts to oversee compliance with requirements pertaining to public disclosures regarding classified contracts and related brochures, promotional sales literature and reports to stockholders, as well as presentations at symposiums, conventions and so forth. Oversight may be accomplished by acquiring and reviewing material which is available upon public request and by random visits to conventions and symposiums that are open to the public.

24. Increased Emphasis on Classification Management

a. The senior DoD official who is delegated the functional responsibility of administering and overseeing the DoD Information Security Program should have ample authority and staff to implement an aggressive and effective program, with particular emphasis on security education and classification management. Quarterly DoD/defense industry regional classification management seminars should be initiated. These seminars will enable responsible policy, procurement, and security officials to remain current with DoD component/industry implementation of established policy and to receive complaints and recommendations for overall classification management improvement. The seminars would also provide for the promulgation of the latest policy developments and concerns, a continuing education and training program for DoD project managers and contractor classification specialists, and for the establishment of more active dialogue between DoD and defense industry.

b. The classification management aspects of the DoD Information Security Program should be subject to a separate study by a panel of experts, to include defense industry representation. The study should particularly emphasize the adequacy of the existing practices and procedures for promulgating and disseminating classification guidance to cleared defense contractors. In addition, the panel should determine whether information developed in the conceptual and research and development stages of a potential program or project is afforded adequate protection against unauthorized disclosure before the assignment of a security classification.

25. Prevention of "Bootlegging" of Classified Material

Security training should be strengthened by focusing attention on the "bootlegging" problem. As a preventive measure, procedures should be established for seeking approval and legitimate transfer of classified material. Moreover, a debriefing specifically addressing "bootlegging" should be administered to all cleared employees before termination of their employment. In addition, each employee should sign a certificate that states he or she possesses no classified material and is aware of the consequences for violating the terms of the certificate. The certificate will be retained for use in the event that the executor is determined to have "bootlegged" classified material. Finally, appropriate sanctions should be established for contractors who knowingly and willingly assume custody of classified material known to have been "bootlegged."

APPENDIX I

Overview of the Defense Industrial Security Program

DEFENSE INDUSTRIAL SECURITY PROGRAM - OVERVIEW

Over the years, the Department of Defense (DoD) has developed a comprehensive Industrial Security Program designed to safeguard classified information released to industry. The current authority for the program is Executive Order (E.O.) 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended by E.O. 10909, January 17, 1961. In addition to the Defense Department, eighteen other Federal agencies and departments use the services and procedures of this program, pursuant to authority granted by E.O. 10865. This is accomplished by an exchange of letters between the Secretary of Defense and the heads of non-DoD departments and agencies (User Agencies) for which the Secretary of Defense is authorized to act in rendering industrial security services. User Agencies include the Office of the Secretary of Defense (OSD) (including all boards, councils, staff and commands); DoD agencies and the Departments of the Army, Navy, and Air Force (including all of their activities); National Aeronautics and Space Administration; General Services Administration; Small Business Administration; National Science Foundation; Environmental Protection Agency; Federal Emergency Management Agency; Federal Reserve Board; General Accounting Office; U.S. Information Agency; U.S. Arms Control and Disarmament Agency; and the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice.

The Deputy Under Secretary of Defense for Policy (DUSD(P)) is responsible for developing and approving of all security policy under the Defense Industrial Security Program (DISP). The DISP is administered by the Director, Defense Investigative Service (DIS). DoD Directive 5220.22 implements E.O. 10865 within the Defense Department and authorizes publication of the "Industrial Security Regulation" (DoD 5220.22-R) and the Industrial Security Manual (DoD 5220.22-M). The "Industrial

Security Regulation" (ISR) sets forth policies, practices, and procedures of the DISP used internally by the DoD to insure maximum uniformity and effectiveness in its application throughout industry.

The DoD Industrial Security Manual (ISM), a companion document to the ISR, contains detailed security requirements to be followed by U.S. contractors entrusted with safeguarding classified information. The ISM is made applicable to industry by management agreement, in concert with the DIS, to the terms of the Department of Defense Security Agreement (DD Form 441), and by direct reference in the "Military Security Requirements" clause in the contract.

The ISR and ISM are written in terms of the most common situation in which contractors have access to classified information in connection with performance of a classified contract; however, they are also applicable to the safeguarding of classified information in connection with all aspects of post-contract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract, such as classified information released pursuant to a User Agency program that a firm, organization, or individual participated in on a voluntary or grant basis. This includes foreign classified information that the U.S. Government is obliged to protect in the interest of national security.

The security policy under the DISP is approved only after coordination with the User Agencies. Proposed changes for policy improvement are initiated within the office of the DUSD(P), by the DIS, by the User Agencies, or at the suggestion of industry. Concerns of industry are usually expressed through the Council of Defense and Space Industry Associations (CODSIA). The CODSIA is given the opportunity to review and comment on proposed changes to the ISM before approval and publication.

Although actual administration of the DISP is assigned to the Director, DIS, the responsibility for security cognizance for all contractors and industrial facilities under the DISP has been assigned to the DIS Deputy Director (Industrial Security). Security cognizance authority has, in turn, been delegated to Regional Directors of Industrial Security for all contractor facilities located within prescribed geographical boundaries. There are eight DIS Directors of Industrial Security located throughout the United States.

At present, the DISP includes nearly 14,000 cleared facilities with about 1,400,000 cleared contractor employees. Furthermore, it is estimated that private industry possesses about 16 million classified documents under the DISP. Worldwide, approximately 800 DIS personnel are assigned to Industrial Security Program related duties and responsibilities, of which approximately 200 of these are engaged in field inspection activities.

Under the DISP, the User Agencies may release classified information to contractors, but only after the management and personnel of the industrial facility have been investigated and a determination has been made that access to and custody of such information is consistent with the national security. An integral part of this determination is to ensure that cleared contractor facilities are sufficiently insulated from foreign ownership, control, and influence. Once cleared, contractor facilities are subject to periodic security inspections by industrial security representatives from the DIS Industrial Security Regional offices (cognizant security offices).

A contractor is not permitted to solicit his own security clearance. In order to be processed for a facility security clearance, the contractor must have an impending need for access to classified information. The prospective contractor must be sponsored by a Government contracting activity or a cleared contractor already engaged in classified contracts or programs who wishes to use the services of the prospective contractor in a capacity that requires access to classified information. This requirement is designed to ensure that investigative resources are not unnecessarily expended and that a facility is not cleared unless there is a valid need for classified access.

Staff personnel at each cognizant security office assist the Director of Industrial Security in administering the various aspects of the DISP. Such functions generally include:

a. Processing facility security clearances for industrial facilities located within the region's geographical area and maintaining such clearances in a current status once granted.

b. Evaluating factors of foreign ownership, control or influence that may be present in the facility.

c. Processing conditions that have changed at the facility since it was initially granted a clearance.

d. Responding to requests for verification of facility clearances and assessing the capabilities of the facility to safeguard classified information.

e. Monitoring international aspects of the program, to include assisting in the arrangement for government-to-

- Provides advice, guidance and assistance on industrial security matters to U.S., foreign and international organization officials. Maintains liaison with such officials on a recurring basis.

- Provides limited classified storage facilities to User Agencies or cleared U.S. contractors. Ensures that material that is not releasable to foreign governments or their citizens is safeguarded within a U.S. Government-controlled activity.

- Assists in the establishment of government-to-government transmission channels between the U.S. and foreign governments. Serves as a conduit for the designated U.S. Government Representative in processing classified material received from a foreign government.

- Conducts industrial security inspections of contractor facilities located overseas on U.S. Government controlled military installations.

In conclusion, the Deputy Under Secretary of Defense (Policy) (DUSD(P)), is the senior DoD official responsible for overall policy guidance and management oversight of the DISP. Staff representatives of the DUSD(P) arrange periodic visits to DIS activities to determine the effectiveness of the operations and adequacy of practices and procedures that are used in the administration of the DISP.

The DISP was functionally transferred from the Defense Logistics Agency to the Defense Investigative Service in October 1980. The DIS was established in 1972 to provide a single centrally directed service within the Department of Defense for conducting personnel security investigations. Today, it is a separate DoD agency headquartered in Washington, D.C.

APPENDIX VIII

The Case of James Harper and Ruby Louise Schuler

(Prepared by the Defense Security Institute)

The Case of James Harper and Ruby Louise Schuler

On May 14, 1984, James Durward Harper was sentenced to life in prison, with a recomendation that he never be paroled. He had pleaded guilty in April to selling classified documents to the Polish Intelligence Service. The material, classified up to Secret, pertained to survivability of the Minuteman missile system and to U.S. defenses against attack by ballistic missiles.

Harper was a self-employed electronics engineer in Mountain View, California. He first became involved with the Poles in 1975 when a business associate, William Bell Hugle, introduced him to Polish agents seeking U.S. electronics technology. Harper was at that time running a small firm which made and marketed the world's first digital stop-watches. He sold technological information to the Poles for several thousand dollars. Harper did not hold a security clearance and had no direct access to classified information.

But in May 1979 Harper began what appears to have been a sort of "business-romance" with a woman named Ruby Louise Schuler. She held a Secret clearance as Executive Secretary to the President of Systems Control, Incorporated (SCI), in Palo Alto, California, a Defense contractor doing research for the U.S. Army Ballistic Missile Defense Advance Technology Center, Huntsville, Alabama. Schuler agreed to provide documents to be copied and sold. Harper contacted Hugle who, in return for a share of the proceeds, arranged a meeting with Polish Intelligence in Warsaw.

Harper conducted a total of a dozen meetings with Polish agents in Warsaw, Vienna and various locatons in Mexico between July 1979 and November 1981. He received approximately

$250,000 for documents whose loss has been rated by Army experts as "beyond calculation."

Harper and Schuler were married in October 1980. She died in June 1983 from complications of cirrhosis of the liver.

James Harper was ultimately arrested in October 1983, partly on the basis of information from a source within the Polish Intelligence Service. But his apprehension was also partly due to his own futile efforts to negotiate immunity and a double-agent role for himself through anonymous contacts with the Central Intelligence Agency and the Federal Bureau of Investigation (FBI). Shortly after his arrest, numerous classified documents were recovered from a safe deposit box in his name in a bank in Tijuana, Mexico.

The case against Harper has now been completed with his sentencing and incarceration. But certain aspects of the investigations remain active. This account is based primarily upon court papers pertaining to the prosecution of Harper, especially affidavits and testimony by the FBI investigators. It is also drawn upon a follow-on inspection of the cleared facility by the Defense Investigative Service.

The most detailed account of Harper's activities was provided by prosecution testimony at a presentencing hearing on April 16, 1984. This hearing did not receive extensive coverage in the press, although more limited information available at the time of Harper's arrest last October was widely reported.

Accompanied by his friend, Mr. Hugle, James Harper sat down on July 17, 1979 in Warsaw across the table from Zdzislaw Przychodzien, known publicly as an official of Polish Ministry of Machine Industry but in fact a lieutenant colonel in the

Polish Intelligence Service and head of an intelligence section of "Wydzial" using the Ministry as cover for collection operations against the West. Przychodzien was fluent in English, having been assigned to the U.S. in the 1970's with the Polish Commercial Office in New York.

Harper described the materials now accessible to him through Louise Schuler at Systems Control, including classified documents pertaining to U.S. strategic forces and ballistic missile defenses. And he provided reproduced excerpts of ten documents. (Enroute to Warsaw he had placed copies of the full documents in a safe deposit box at the Citibank in Paris.)

Przychodzien was very interested in the material. He promised generous payment, although he demurred at the American's initial asking price of $1 million. Also discussed at this July meeting was other materials available to Harper including computer data base tapes obtainable through his contacts in Silicon Valley.

Harper and Hugle agreed to meet with Przychodzien again in Vienna the following October. On that occasion, Harper delivered full-text copies of the ten documents which Przychodzien had previewed earlier. He also provided excerpts of additional documents. But a disagreement arose over the matter of payment which caused the meeting break-up. Harper was unsure of his position with Przychodzien. It appeared that the Poles were not as interested in the classified Defense documents from SCI as he had originally thought, so, upon his return to California, he buried them in an out-of-the-way location in the San Joaquin River delta near Stockton--just for safe-keeping in case a buyer could later be found.

At this point, Harper wanted nothing further to do with Hugle, but he was able to reestablish contact with Przychodzien through a friend in Switzerland, and he returned to Warsaw in May 1980 with the Silicon Valley data base tapes and without any classified documents. But it was the classified ballistic missile material that Przychodzien really wanted. The intelligence officer paid $10,000 for the ten documents delivered at the meeting in Vienna and urged Harper to come back with all of the Defense documents he could get his hands on.

So Harper went back to the delta, dug up his "stash" and transported the additional documents to Warsaw (via Vienna and Geneva) the following month (June 1980). Harper later estimated that this second delivery of classified reports weighed about 100 pounds. The documents were somewhat the worse for their seven-month interment on the banks of the San Joaquin River. But Przychodzien's people worked through the night of June 5 to separate the matted pages and restore the materials to decipherable condition.

On June 6, the documents were brought to the Soviet Embassy where a team of 20 KGB experts, flown in specially from Moscow, declared them to be genuine and extremely valuable. Harper was paid $100,000 on this occasion. A month later Przychodzien and his unit received a commendation for their efforts, directly from KGB Chairman Yuri Andropov.

Harper next returend to Warsaw in September 1980, this time bringing along a document register for the safe in his wife's office, i.e., an inventory of all documents in the SCI president's security container. The Poles selected several items for purchase and Harper delivered them during visits to Warsaw in October and November 1980, receiving $20,000 in payment.

During the November meeting with Przychodzien, Harper was instructed to meet next time in Mexico City with a Polish agent whom he knew only as "Jacques."

The first meeting with Jacques took place as agreed at the cashier cage of the Museum of Anthropology on December 14, 1980. Harper brought no documents, treating the occasion as a dry run to establish contact and "get the feel of the city." Jacques paid him $10,000 anyway, and at the next encounter in the same city two months later Harper brought nine Secret documents and received $60,000.

Following one more transaction with Jacques (eight classified documents and excerpts for 30 more, in return for $50,000), Harper told the agent in September 1981 that he was dissatisfied with the payments he was receiving. He brought no documents to the September meeting in Guadalajara, and received no payment, although Jacques had brought along $30,000 for the 30 documents previewed last time in extract. It was agreed that Harper would go back to Warsaw to work out his complaints with Przychodzien directly.

This was in fact the end of Harper's active dealings with the Poles. He made a trip to Warsaw in November 1981 and spoke with Przychodzien, but he remained dissatisfied with the payments offered and no further contacts ensued. Before going to Warsaw, Harper had driven with Louise to Tijuana and placed his remaining collection of classified documents in a safe deposit box where they remained until retrieved by the FBI, with Harper's cooperaton, following his arrest.

These were, in fact, the last documents available to Harper, since Louise lost her clearance in August 1981, not due to any suspicion of her activities, but rather due to acquisition of her company by a foreign firm. Under an arrangement approved by the DoD, SCI's Defense contracts have been retained by a "spin-off" company insulated from the parent by a stock proxy agreement. The facility clearance for this subsidiary was later upgraded from Secret to Top Secret. But Ruby Schuler remained an employee of the original SCI organization, now under British ownership, and her Secret clearance was administratively terminated as a result.

She died June 1983 of cirrhosis of the liver. Her death certificate lists "alcoholism" as a "secondary cause" of death.

In September 1981, at the time he was becoming increasingly unhappy about his exchanges with the Poles, Harper contacted attorney William Dougherty requesting that Dougherty act as go-between in negotiations with the CIA and FBI. Harper wanted to arrange immunity from prosecution in exchange for information on his activities and services as a double agent. While concealing his identity from the lawyer, he provided detailed written and tape-recorded accounts of his espionage activities through Dougherty to the Government. This continued for two years until Harper's ultimate arrest, although the Government showed no willingness to agree to his terms.

Investigators succeeded in positively identifying him in March 1983. He was immediately placed under surveillance at his home in Mountain View, California, where he was at that time living with Louise. Wiretaps were also authorized and installed on their telephone. Investigators were able to learn the location of a storage locker where Harper kept records of his activities. They also learned he was planning overseas travel and was again in contact with the Swiss friend who had arranged earlier meetings with Przychodzien.

He was arrested on October 15, 1983, forestalling any chance that he would turn over his remaining documents.

One lesson of this case is unmistakable confirmation of the intimate ties between Warsaw Pact intelligence services and the Soviet KGB. It is clear not only that the Polish Intelligence Service works closely with the KGB, but that they in fact work for the KGB. When Harper brought his main installment of documents to Warsaw in June 1980, the Poles spent the night putting the pages in order, but once collated, the materials were immediately turned over to the Soviets for evaluation and analysis.

Harper has stated to the FBI that the tasking presented him by the Polish agents was derived from a "master shopping list" provided by the Soviets. And this has been confirmed by the Polish intelligence officer who served as a source in breaking the Harper case. The source has confirmed that Polish agents respond directly to detailed tasking from the KGB, with military collection as a top priority.

The Polish source was aware of Harper's activities, although he did not know Harper's identity. Przychodzien had told him of the initial meetings with an American, fitting Harper's description, who had access to ballistic missile information. And he even recalled seeing a phone message from Hugle written on Przychodzien's desk calendar at the time of those first meetings in October 1979. This inside information confirmed the authenticity of Harper's accounts once his anonymous statements began coming in.

Information so far available does not reveal any major security deficiencies at SCI which can be identified as contributing directly to Harper's and Schuler's activities. She apparently removed the documents from the facility to be reproduced at home on a paper copier which Harper had bought for the purpose. As in most facilities, governmental or industrial, there were no searches at the exits to prevent removal of classified material.

Schuler was noted in the facility during evenings and weekends. On at least one occasion Harper was with her. But this was not a violation since he was escorted -- by Schuler! Unexplained off-hours activity has often been highlighted as a possible indication of espionage, and this is another case in point.

As a result of the case, the company has centralized its classified document storage at one location under direct control of the security officer (something which would obviously not be possible for a larger facility), and they have implemented tighter personnel access controls for nonworking hours.

There are some indicators that certain adverse information regarding Louise Schuler was known to co-workers and company officials and was not reported. She was, first of all, an alcoholic and ultimately died of complicatons from that disorder. Quotations in the press indicate that co-workers were aware that she carried vodka in her purse and drank on the job. An inquiry into that issue might have revealed some indication of her illicit activities, or possibly exerted some deterrent effect.

In addition, a former official of the company, also a cleared individual, had a close involvement with Louise during much of the period in question, and he was aware not only of her drinking, but also of her unexplained income. She does not seem to have flaunted her ill-gotten gains in a public sort of way, and most co-workers would have had no occasion to notice anything out of the ordinary. But the company executive was with her on at least one occasion when she placed a large stack of $100 bills in a safe deposit box at a local bank. He did not report this either at the time or when later interviewed by the FBI. His security clearance (he is now with another cleared company) has been suspended pending resolution of his possible involvement in the case.

APPENDIX IX

The Case of William Bell and Marian Zacharski

(Prepared by the Defense Security Institute)

The Case of William Bell and Marian Zacharski

Marian Zacharski arrived in Los Angeles from Poland in late 1976. He was assigned as West Coast Branch Manager for the Polish American Machinery Company (POLAMCO), a U.S. incorporated firm serving as marketing arm for the Polish trade agency, Metal Export.

But machinery was not Zacharski's only business. He was also covertly assigned by the Polish Intelligence Service to spot and recruit agents within California's aerospace industry. And he was for a time highly successful in both of his occupations. By early 1981 (at the age of 29), he has been appointed president of POLAMCO, and he had recruited at least one agent with access to important classified weapons information and technology.

Thereafter, Zacharski's fortunes took a turn for the worse, and by the end of 1981, he was serving a life sentence for espionage against the United States -- but not before doing both a lot of good for Polish exports and a lot of harm to U.S national security.

William Bell was Zacharski's agent. He was born in Seattle, Washington, on May 14, 1920. He was employed as an engineer with Hughes Aircraft Company and met the Polish businessman in 1977 at the Cross Creek Apartments in Playa del Ray where both were residents. The two shared an interest in tennis as well as a common concern with the aerospace industry, where Zacharski sold much of his industrial equipment.

After almost a year of purely social and recreational contacts, Zacharski began to ask Bell for unclassified literature from work. Then he asked for "interesting" material and received first Confidential, then Secret documents to look over. He paid Bell lavishly for his minimal "consulting" work. And when Zacharski proposed that Bell, for additional thousands of dollars, photograph clasified documents and carry them to Europe to meet other Polish representatives, Bell was ready to go along. Soon he felt "over his head" and too committed to back out. William Bell is now in prison, serving an eight-year sentence.

Zacharski's recruitment approach was a standard one. It should be as familiar and, hence, as ineffective as attempts to sell shares in the Brooklyn Bridge. But Bell's susceptibility was not the result of tender years, or slim experience or lack of education, training or intelligence. He was 57 years old when he met Zacharski, with 25 years in defense work, a B.S. in applied physics from UCLA and two overseas tours with his company.

Bell had been briefed on the threat of hostile intelligence services, but he did not recognize the classic approach when he encountered it in real life. He did not believe that it could actually be happening to him, that this amiable Polish tennis buff (who reminded him of his estranged older son) could possibly be anything other than what he appeared to be.

Marian Zacharski was arrested for espionage in June 1981 and went to trial in October. He was convicted largely on the basis of William Bell's testimony against him, and Bell's lighter sentence was based in part upon consideration of his cooperation with the government in the final stages of the investigation and the trial. This account of the Bell/Zacharski espionage case is based primarily upon the transcript of Zacharski's trial. It also draws upon Bell's testimony in May 1982 before the Senate Permanent Subcommittee on Investigations.

In the fall of 1977, when he was first introduced to Marian Zacharski at the swimming pool of the Cross Creek Apartments, William Bell had recently returned to Los Angeles from an assignment in Brussels as Manager of European Operations for the Radar Systems Group, Hughes International Corporation. He was now a Project Manager in the Advanced Systems Divsion, Radar Systems Group at the main Hughes facility in Los Angeles.

Bell held a Secret security clearance and was responsible, as he later testified, for "development and promotion of the radar fire control product line of tank vehicles." He had been with Hughes since graduation from UCLA in 1952, employed entirely at the Los Angeles facility except for two European assignments (in mid-1960's and from 1974 to 1976).

In his Senate testimony, Bell stated that these overseas assignments had been "financial nightmares" for him, "although they are touted as glamorous and lucrative." Upon his return in 1976, he recalled, he was "pursued by four separate Internal Revenue Service offices for back taxes on disallowed deductions primarily arising out of my overseas assignments." The year of 1976 was in fact a low point in Bell's life for a number of reasons. He was divorced from his wife after 29 years of marriage ("in an extended proceeding") and was faced with alimony payments of $200 per week. His accumulated debts forced him to file bankruptcy in July 1976. During the previous year, Bell's family had suffered a tragic loss when his 19 year old son died in a camping accident in Mexico.

In addition to financial hardship, divorce and personal tragedy, Bell also later recalled feeling "like an outsider" upon his return to the Los Angeles plant. "I returned from Europe to find a younger group at Hughes and I (was) shunted off to a quiet back room." But regardless of any disappointment with his assignment, Bell was in fact given major responsibilities for development of advanced weapons systems -- a fact which Marian Zacharski was quick to learn.

When he met Zacharski in 1977, Bell was attempting to make a new start. He had remarried ("to a young Belgian citizen," formerly his secretary overseas) and had taken up residence with her and her six year old son at the Cross Creek Apartments. He was making a gradual financial recovery (although alimony, taxes and debts still put a strain on his $35,000 income). And he found comfort in the companionship of a close friend:

> "Zacharski and his wife moved into the apartment complex and I began to play tennis (with him) on a daily basis. He slowly became my best friend. He was about the age of my oldest son who had been close to his mother and quite distant from me since our divorce."

Marian "made friends easily," Bell recalled. The two couples socialized frequently, both by themselves and with an informal "little United Nations," a social group at the complex consisting of couples one or both of whom were foreign nationals. And the two men found common professional interests as well. Zacharski was a skilled and successful salesman of industrial equipment and the California aerospace industry was one of his principal sales targets. He naturally discussed the aerospace business with his tennis partner and in about mid-1978, he asked Bell for help in making contacts at Hughes and other companies in the field.

Bell gave Zacharski's name to a purchasing manager at Hughes and also contacted people at Lockheed and Northrop. And for this, Zacharski paid him approximately $5,000. At the trial, the cross-examining attorney wondered why Bell had not been suspicious of such generosity. He had been, he claimed, though evidently only temporarily. "To receive four or five thousand dollars for doing practically nothing made me very suspicious."

> Q: It also made you very glad, did it not, Mr. Bell?
> A: It sure did. I needed the money.

Bell and Zacharski discussed the possibility that Bell might be permanently retained by POLAMCO as a "consulting engineer" and sales advisor, although the terms of the arrangement were left studiously indefinite ("I was working, in a way, and talked about working as a consultant for POLAMCO..."). Bell began again around mid-1978, to provide printed material from the office, to help Zacharski keep abreast of sales opportunities. It started out (with) simple things," Bell later told the grand jury, "like the Hughes News," the company newspaper.

Then came documents of more technical substance. He brought Zacharski copies of the Hughes "Vector," a technically-oriented publicity sheet on company programs. Zacharski had specifically requested these openly-published materials. But then Bell began to volunteer materials in response to Zacharski's general expressions of interests. "I could tell from our conversatons that they were things that he would like to see." "We would be talking about it at the tennis court -- unclassified documents in the beginning."

During the summer of 1978, he provided Marian with several documents "related to items that were machined." These were unclasified, at least for the most part, but "there was possibly one Confidential .... I'm not certain." Bell has never been sure of exactly when he first showed Zacharski a Confidential document -- or just which or how many such documents he had compromised.

He may also have been uncertain in his grasp of security requirements for the handling of Confidential material, as indicated by this courtroom exchange between Bell and prosecutor Robert Brewer:

> Q: Would that (taking documents home) be a violaton of ... security policy?
>
> A: Not a Confidential document no. You can bring confidential documents home. You cannot bring secret documents home.

The Secret documents which Bell compromised can be more reliably identified since the company maintained accountability records for them (not required by the Industrial Security Manual for Confidential). Bell determined that his first transfer of Secret material occurred in October or November of 1978 when he lent Zacharski (at the tennis court) Copy No. 8 of the "Proposal for a Covert All-Weather Gun System, Executive Summary, Volume I." Bell was the author of this material. He wanted Zacharski to understand his role at Hughes and he wanted to impress him with his work. "I was proud of it," he said of the Executive Summary, "and I gave it to him." Later, Bell turned over an unclassified document on the same subject and stamped it Secret "to make it look more important."

The Covert All-Weather Gun System ("CAWGS") was the primary development project under Bell's technical management at that time. It envisioned the application to tanks of the Low Probability of Intercept Radar ("LPIR") or "quiet radar." LPIR utilizes a disguised radar signal which is difficult for enemy targets to identify as radar; they are thus prevented from taking evasive action or using the radar signal for directing return fire. The CAWG, subsequently redesignated the Dual Purpose Weapon System or "DPWS" (to be used against both aircraft and other tanks), was Bell's main responsibility throughout his relationship with Zacharski. It was, according to trial testimony, the principal program compromised by his espionage activities.

It was announced in mid-1978 that the Cross Creek Apartments would be converted to condominiums. Bell and his wife wanted to remain, but he was worried that he could not make the down payment required to purchase his unit. His friend Zacharski said he might be able to help. And in February 1979, he provided Bell with $12,000 in two payments handed over in envelopes at the door of Bell's apartment. They were speedy and uncomplicated transactions, as Bell later testified: "Q: Did you say anything to him? A: 'Thanks.'"

He used the money for the condominium payment and for back taxes. He assumed that the money was from POLAMCO's "marketing" fund. And he credited Marian's good will with inspiring this generosity. "I thought we were good friends and I knew he would like me to stay in the apartment complex. I wanted the condominium and I accepted the money."

Bell still thought it was in connection with "consulting" activities when Zacharski suggested, in the summer of 1979, that he travel to Europe to meet certain unidentified Polish representatives ("whom I thought would be POLAMCO people"). He was asked to photograph documents from work and bring the film with him to the meeting in Innsbruck, Austria. Marian had earlier given Bell a Canon movie camera, which turned out to have a frame-by-frame capability ideal for photographing documents. He provided a tripod and special film and instructed Bell in using the camera in his bedroom.

William Bell departed on the first of four overseas "missions" on November 26, 1979. Marian gave him about $2500 for expenses, although Bell's wife was an airline flight attendant and his trans-Atlantic fare was $18. On the morning of November 30, he went to a predesignated restaurant in Innsbruck and was met by a man who introduced himself as "Paul" and asked "are you a friend of Marian's?" -- the agreed upon recognition signal. The two left the restaurant and entered a car driven by another man (name not recalled) and drove to the outskirts of Innsbruck.

Bell handed over his film and the three men discussed Bell's work, the types of information he should attempt to collect and the need for secrecy and security. At one point Bell was shown a picture of his wife and son. "He (Paul) told me that I had a lovely family. Then he said that our security depended upon each other and that if anybody got out of line that he'd take care of them." The Poles did not dwell on the point, but Bell clearly perceived an "implied threat" in Paul's words. Before leaving Innsbruck, he received $7,000 and agreed to another meeting in the same city in May 1980.

When he returned to Los Angeles, Bell received an additional list of desired collection targets from Zacharski. On this and other occasions he was surprised at Zacharski's highly specific knowledge of system designations and even particular document numbers.

> Q: And did you ever ask Mr. Zacharski where he obtained those numbers?
>
> A: Yes.

Q: What did he say, if anything?

A: He didn't answer me. He just smiled.

By now, at the end of 1979, Bell could no longer maintain the illusion that he was involved in a (more or less) innocent consulting arrangement with POLAMCO. It was clear, as he testified, that he was "conducting espionage" for "agents or offices of the Polish Intelligence Service." And Zacharski himself dropped any such pretense after that time. He made no more requests for assistance in promoting machine tools.

Bell took three more trips to Europe, meeting with one or both of the Polish operatives at Innsbruck in May 1980, at Linz (Austria) in October 1980 and at Geneva in April 1981. Prior to each meeting, he photographed several documents with the movie camera in his apartment (when his wife was away). At the Innsbruck meetings, he provided film of unclassified and Confidential documents. At Linz and Geneva, he turned over copies of Secret material related to the DPWS and LPIR systems. He continued to receive substantial payments, in bills and in gold, from both Zacharski and the handlers overseas.

After Geneva, Bell's next meeting with the Poles was to be in Mexico City. He was uneasy about transacting his business there, he testified, in part because "Mexico City is where a spy was caught, I don't recall his name." The name, of course, was Daulton Lee, accomplice of TRW spy Christopher Boyce. But Bell was relieved of the necessity of following Lee's footsteps to Mexico. He was called to Hughes security on June 23, 1981 to be questioned by the FBI. At the trial, Special Agent James Reid recalled the crucial point of the interrogation as follows:

(Reid): I showed Mr. Bell a translation of a Polish newspaper article which indicated an individual who had been assigned to the U.N. in New York had defected to the United States Government. I then explained to Mr. Bell that this individual had in fact defected, and that he had been providing the FBI with information concerning activities of the Polish Intelligence Service in this country.

Q: What if anything did Mr. Bell say?

A: Mr. Bell asked, "Did he mention me?" And then without waiting for an answer, he said, "this is very serious. I would like to talk to an attorney."

(Reid told Bell that he could talk with a government attorney or make a telephone call to an attorney of his own.)

Q: And after you said that, what happened?

A: Well, at that point Mr. Bell physically slumped in his chair and he said, "I did it. I do not need an attorney."

Bell signed a confession and agreed to cooperate in the further investigation of Zacharski. On June 28, he was fitted with a hidden recording device when he met with Marian on the apartment grounds to discuss further payments and certain sensitive programs at Hughes which Zacharski was interested in targeting. Zacharski was arrested shortly thereafter.

The Lessons

The Bell case, like any other espionage case, has its unique and peculiar elements. But it is, by and large, a "text-book" case which confirms many of the long-standing precepts of counterintelligence, as well as patterns derived from recent espionage cases.

Financial gain was Bell's primary motivaton. This is typical of most recent cases, and his testimony was quite clear on the point. Politics or ideology did not play a part:

> Q: You are not, in other words, a secret Polish patriot?
>
> A: No I am not.

The motivation was primarily mercenary. "Mr. Zacharski had found a fool that needed money. I had a weak spot. He took advantage of me." Bell also cited the veiled threats from "Paul." This played some part in his thinking and discouraged him from pulling out once he was involved, but "the motive was always money." ("Q: Was it worth it? A: No, absolutely not.")

Financial difficulties and other personal problems were an important cause of Bell's susceptibility to recruitment. From his trial testimony, it appears that Bell faced the kind of difficulties which everyone encounters at some time during life, although the coincidence of several misfortunes in quick succession clearly contributed to an imbalance in judgment. Withdrawl of clearances in cases like this might generally be considered both cruel and unusual. But certainly whatever positive assistance or counselling an organization might provide to employees in trouble, combined with an active program of defensive security training, will help to ensure that a person like Bell is not so choice a target for a person like Zacharski.

Job dissatisfaction or some element of grudge against the company or the U.S. government have figured as predisposing elements in several recent cases (Boyce, Kampiles, Edwin Moore, etc.). Bell's remarks display some signs of disgruntlement with Hughes. The European assignments were not as "glamorous and lucrative" as they were "touted" to be; he felt like an "outsider" among the younger personnel at the Los Angeles plant -- and so forth. But here again Bell's difficulties were of a rather ordinary sort, providing no obvious warning of an employee who was ready to take desperate measures.

Several attempts have been made in recent years to draw up a behavioral profile of the typical spy, to identify the patterns of activity which are characteristic of espionage in progress. Bell's is presumably one of the cases which underlies this analysis and his activities do in fact lend credence to several of the major espionage indicators. Early reporting of suspicious behavior may help to halt an espionage operaton before irreparable damage is done.

Unexplained affluence is well known as a possible tip-off to ongoing espionage and certainly Bell received a substantial increase in income from his illicit activities. His estimates of the total amount varied widely, from $470,000 to $170,000. Payments specifically cited during the trial were totalled to between $101,000 and $103,000.

Bell spent or invested most of the money, although some of the gold remained unconverted at the time of his arrest and was confiscated by the government. His testimony indicates that he was relatively conservative in his use of the funds, and even the luxury items cited -- a "red Cadillac," a $2000 necklace for his wife and a brief vacation to Rio de Janeiro --would not necessarily appear extravagant for a family with an income of $52,000 (in 1980, $40,000, his wife, $12,000). Much has been made in press coverage regarding the "young stewardess" angle in the case, but there is no indication that Bell's second wife either contributed to his financial setbacks or drove him to seek new income in support of an inflated lifestyle. (And she was not in fact an airline flight attendant when she met and married him but entered training in January 1979.)

Bell's windfall earnings were directed not to high living but primarily to hastening his recovery from bankruptcy. His was a case not so much of unexplained affluence as of unexpected solvency. Any major alteration in financial circumstances may be of significance when personnel with access to classified information are involved.

Attempts to gain unauthorized access to classified information (e.g., beyond ligitimate need to know) are often characteristic of diligent spies, but Bell seems to have avoided this pitfall. He was apparently a cautious (or lazy) agent and did not seek out information beyond his assigned projects. The major compromises confirmed at the trial (LPIR, DPWS) fall within the scope of his primary duties as a project manager.

Removal of classified material from the facility is a more or less inevitable accompaniment to spying, and certainly Bell took some risks in this regard. When he carried documents home to be photographed, he was vulnerable to detection since Hughes had a policy of random searches at the plant exits. Either Bell was lucky in his timing or he was somehow able to anticipate the searches. In any case, he was never caught in the act.

Foreign travel, on a regular basis and without sufficient explanation, is another "tell-tale sign" displayed by Bell and one which evidently contributed to his detection. His trips to Europe were partially legitimized by company business and family visits. But testimony (by Bell himself and by a Hughes security official) indicates that his overseas travel -- and, on one occasion, incomplete reporting of his itinerary -- was a factor which helped to place him under suspicion.

So Bell confirms, to some degree, certain of the behavioral patterns associated with previous cases of this kind. Financial difficulties and job-related dissatisfaction can predispose an individual to espionage. Unexplained income, unauthorized removal of documents and unexplained foreign travel may be indicators that espionage activity is underway. But the case also confirms the difficulty of applying this sort of preventive counterintelligence to real-world situations, without the benefit of "20/20 hindsight." The real "ounce of prevention" would have involved measures to forestall Bell's recruitment in the first place. And there is good reason to think that this could have been done -- with the infusion of a little more awareness.

This presupposes that Bell was genuinely unaware, during the initial stages, of what Zacharski was up to. A more cynical view might suppose that he knew exactly what was happening all along and complied with Zacharski's wishes, from the beginning, with his eyes wide open. But those who investigated and prosecuted Bell are inclined to accept his account of the evolution of the case. And Bell has testified that, when he returned to the state-side facility from Brussels, he assumed that his worries were over where hostile intelligence activities were concerned. "When you are sent to Europe," he told the Senate Subcommittee, "you are told to expect attempts by foreign spies, but whoever would expect it to happen here at home?"

He received the required briefings and signed the required forms upon rejoining the Los Angeles organization, but apparently treated them as a matter of insignificant routine. A "Security Briefing and Termination Statement" was introduced in evidence at the trial, and he acknowledged having seen it: "I recall signing the normal form you signed when you hire into the company.... There are many forms you sign and I am sure that was one of them."

"Whoever would expect it to happen here at home?" It was in this innocent frame of mind that Bell initially made the acquaintance of the Polish machinery salesman and then agreed (in fact eagerly sought) to serve as a consultant for POLAMCO, an arrangement which included providing inside information on his company. The delusion persisted right up to his first overseas visit:

> Even as I went to Innsbruck, Austria, I was rationalizing and kidding myself that the persons I would meet were representatives of POLAMCO, that this was just the kind of industrial espionage that goes on all the time.

After his return from Innsbruck, Bell knew exactly what he was doing and exactly what had been done to him. Why he did not extricate himself at that point is a complex psychological question involving a confluence of material inducements, Zacharski's personal magnetism and "Paul's" implicit menace. For whatever reason, Bell now felt genuinely trapped. He told the Senators after his conviction: "There is little left of my life now but I feel I am freer in prison than I was with Zacharski."

Clearly, there was more to this entrapment than simple monetary temptation. And we must not take too literally Bell's own statement that he was "a fool that needed money." A fool he may have been and he was certainly hungry for cash. But too much stress on Bell's foolishness can lead us to ignore Zacharski's skill. Preoccupation with financial motives, moreover, can obscure the fact that many months of cultivation preceded the first mention of money between Zacharski and Bell. We must not ignore the subtle but powerful psychological influences which reinforced the material incentives once offered and laid the groundwork for Bell's receptivity, by creating a willingness to regard Zacharski's offers as well-intentioned, as motivated by friendship and good will.

Bell's recruitment was the result (not necessarily the only result) of a carefully planned and orchestrated intelligence operation. As the focal point for this operation, Zacharski was provided with the best possible cover for his activities, a cloak of propriety calculated to inspire the least possible suspicion. To begin with, his nationality was in his favor. As a citizen of an Eastern European country, he would not present the same threatening image as a Soviet national -- although there can be no doubt that the information he collected was to be shared with Poland's Warsaw Pact ally. (It might be recalled in this connection that during the year Zacharski arrived, 1976, a Presidential candidate had come very close to declaring Poland a member of the free world!)

In addition, he was provided with a commercial rather than a diplomatic position. He was employed, in effect, by the Polish government, but as a salesman of industrial equipment he assumed an image which was less official and hence, again, less threatening. In addition, he was exempt from travel restrictions imposed upon diplomats from communist countries and had more flexibility of movement and greater access to U.S.

industrial facilities and personnel. Of course, commercial status carried with it a certain disadvantage: no diplomatic immunity. Zacharski is no duobt now hoping to be exchanged for someone imprisoned in the Soviet bloc, but there have been no indications that a swap is contemplated.

Once fitted with suitable camouflage, Zacharski was introduced into a promising hunting ground, the technology-rich area of Los Angeles, California. He moved into an apartment complex where many executives and engineers of aerospace companies were residents. And he set to work.

Having met William Bell, as he must have met many others in similar professional positions, and having decided to proceed with cultivation, Zacharski worked with extreme caution and practiced subtlety. He was a skilled salesman and master persuader and well equipped for his task.

Bell testified that they first met in Autumn 1977. He could recall no requests of any kind from Zacharski until mid-1978. So Zacharski spent the better part of an entire year simply making friends with his prospect, insinuating himself into his personal life, meeting and befriending his family, assessing his character traits (and flaws), learning his likes and dislikes (and sharing them), discerning his weaknesses and above all his needs.

Only after many months of this did he begin seeking active assistance from Bell and overtly feeding his desire for money. Cornelius G. Sullivan, a former counterintelligence agent with the FBI, testified at the trial that this is a crucial "dividing line" in the process of developing an agent, the boundary between a simple social relationship and one involving overt exchange. This "barrier" is typically overcome, he said, by first requesting unclassified and seemingly innocent items -- and this of course is the approach which Zacharski adopted.

There is also a second dividing line -- between providing innocent, public materials and handing over restricted, sensitive and/or classified items. Zacharski used the "consulting" process to bridge the barrier between legal successful strategy. It was so effective in fact that Bell aparently volunteered the first transfers of classified material on his own initiative.

Offering the prospect of a consulting arrangement, as a prelude to espionage, proved successful in this case for a number of reasons. The promise of additional income appealed to Bell's financial hunger, of course. And it must also have appealed to his entirely normal professional vanity to be asked to lend his technical expertise and the benefit of his contacts in the industry. Because the arrangement was obviously improper to a degree, it introduced a surreptitious element into the Zacharski/Bell relationship and helped to ease Bell toward a fully clandelstine role as a full-fledged spy. (Bell explained his additional income to his wife as coming from work for a Swiss aircraft firm. He asked her to be discreet about the arrangement, stating that Hughes would not approve of his consulting for a competitive firm.)

Perhaps above all the consulting arrangement permitted Zacharski to deceive Bell, and Bell to deceive himself, into regarding the initial compromises of national security information as a venial sort of "industrial espionage." "Within the avionics industry," Bell told the Senate Subcommittee, "It is a common practice for all companies to obtain the secrets of their competitors by the same techniques Zacharski used with me."

He thought of POLAMCO as "an American company." They had offered him a job which would be "the solution to all my problems." And providing them with inside information from Hughes would only be adhering to the common practices of the industry, as he interpreted them:

> An engineer for one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work and this is normally done without regard to security classification....

Whether or not Bell accurately describes a common practice, he certainly does reflect a common attitude -- "Everybody's Doing It." Zacharski exploited this attitude and used the consulting ploy to ease Bell almost imperceptibly into his initial ventures in the illegal exchange of information. After that, Bell felt that it was too late to back out, and it was indeed too late to prevent some damage to the national security, since some damage had already been done.

APPENDIX X

The Case of Christopher John Boyce

(Prepared by the Defense Security Institute)

The Case of Christopher John Boyce

Christopher Boyce's case involves a program outside the Defense Industrial Security Program and thus only a brief synopsis is provided.

Christopher Boyce was an employee of TRW, Incorporated, in Redondo Beach, California. From 1975 to 1977 he worked as a security clerk in a "black vault" operated at the facility in conjunction with a CIA contract.

Boyce eventually entered into a scheme with his boyhood friend, Daulton Lee, whereby Boyce would remove classified documents from the vault, photograph them, and Lee, in turn, would sell them to the Soviets at their embassy in Mexico City. Eventually, Lee was taken into custody for acting suspicious outside the Soviet Embassy. Mexican authorities discovered clasified material in Lee's possession. Lee, in turn, implicated Boyce.

Ironically, Boyce had already resigned his position at TRW and, at the behest of his Soviet mentors, planned to go back to college and eventually obtain a sensitive government job. Presumably, he would then continue his espionage activities on behalf of the Soviet Union.

Boyce and Lee were arrested by the FBI in January 1977 and charged with selling secrets to Soviet Agents. Both eventually were convicted with Lee being sentenced to life and Boyce being sentenced to 40 years in prison. Incidentally, Boyce escaped from Federal prison in January 1980 and was not recaptured until November 1981.

EXHIBIT NO. 3

Congressional Research Service
The Library of Congress

Washington, D.C. 20540

November 2, 1984

TO : Senate Permanent Subcommittee on Investigations
Attention: Eleanor Hill

FROM : American Law Division

SUBJECT: The Impact of Case Law and Privacy Law on the Federal Employee Loyalty - Security Program

The federal loyalty - security program, under which employees and applicants for employment are subjected to loyalty qualifications to insure that their employment poses no danger to national security, began as a systematic program after World War II. Loyalty qualifications (at both the state and federal level) usually took the form of loyalty oaths and background investigation and screening of employees and applicants.[1/] This memorandum briefly discusses the charges of critics that the federal program has been rendered ineffective by court decisions and restrictive privacy and information disclosure laws. It is limited to a discussion of case law and statutes that have been cited as having undermined the program. Other factors have also been identified as contributing to the present state of the loyalty - security program. These have been surveyed in the critical literature and are not treated here.[2/] Finally, this memorandum focuses on the loyalty aspect of the

---

1/ See generally, Dwoskin, The Rights of the Public Employee 165-213 (1978); Emerson, Haber, Dorsen, Political and Civil Rights in the United States, vol. 1, 202 (1976).

2/ For discussion of the cases and statutes that have had an impact on the program as well as other factors affecting the program see, Lewy, The Federal Loyalty - Security Program -- The Need for Reform (American Enterprise Institute 1983); Martin, The Erosion of the Federal Employee Security Program: A Critique, printed in Hearing on Government Files: Retention or Destruction Before a Subcommittee of Senate Judiciary Comm., 97th Cong., 1st Sess. 49 (1981); Committee Print, The Erosion of Law
(continued)

program. The rubric "loyalty - security" has come to be an umbrella term embracing not only what is traditionally viewed as loyalty but also general employment suitability factors such as competence, criminal history and character deficiencies.

I.

The cases most prominently discussed in the loyalty - security context are those that have enunciated the permissible scope of inquiry into an employment applicant's political beliefs. The test that has emerged is that the government "may not subject a person to a civil disability for mere membership in a particular organization; at most, it may do so for membership in a subversive organization with knowledge of its unlawful purposes and specific intent to further those purposes." Cummings v. Hampton, 485 F. 2d 1153, 1154 (9th Cir. 1973); see also, Baird v. State Bar of Arizona, 401 U.S. 1 (1971). Furthermore, "the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." Brandenburg v. Ohio, 395 U.S. 444, 447 (1969). Thus, courts have struck down inquiries into mere membership in assertedly subversive organizations or employment restrictions linked solely to membership without the specific intent to further the illegal aims of the organization. United States v. Robel, 389 U.S. 258 (1967); Keyishian v. Board of Regents, 385 U.S. 589 (1967); Stewart v. Washington, 301 F. Supp. 610 (D.D.C. 1969) (holding 5 U.S.C. 7311's restrictions on federal and D.C. employment based on advocacy and organization membership unconstitutional); Cummings

---

(continued) Enforcement Intelligence and Its Impact on the Public Security, Senate Judiciary Comm., 95th Cong., 2d Sess. 124 (1978). See also, Hearing on Federal Personnel Security Background Investigations Before a Subcomm. of House Post Office and Civil Service Comm., 96th Cong., 2d Sess. (1980).

v. Hampton, supra (Veterans Administration employment questionnaire struck down); Shapiro v. Roudebush, 413 F. Supp. 1177 (D. Mass. 1976) (similar CSC questions invalidated); Ozonoff v. Berzak, No. 83-1850 (1st Cir. Sept. 21, 1984) (loyalty provisions in E.O. 10422 governing employment of Americans in international organizations struck down). The Court in Cole v. Young, 351 U.S. 536 (1956) also invalidated summary suspension and unreviewable termination of federal employees under a system that proscribed mere knowing membership in certain organizations and included advocacy of abstract doctrine as a basis for termination.

Precision of regulation has been demanded in this area touching on protected First Amendment activity. Restrictions on using mere associational membership as a criterion for employability and proscribing advocacy removed from an imminent lawless result have been intended to insure that persons will not be put to the task of restricting their political conduct to that which is unquestionably safe. See, Baggett v. Bullit, 377 U.S. 360 (1964). Thus, vague or overbroad loyalty oaths may not be employed.[3/] Broad inquiries into associational ties unrelated to the nature of the membership also may pose constitutional problems.

The line of cases from Cole v. Young to the recent Court of Appeals decision in Ozonoff has, however, recognized that the question of overbreadth of inquiry into the activities of applicants for employment must, in the words of the Ozonoff court, be "measured in light of whatever special job-related security requirements that governmental security or foreign policy needs may reasonably dictate..." Thus, the Court in Cole struck down the extension of summary suspension and unreviewable

---

[3/] The Court has upheld a loyalty oath for public employment in which the oath taker swears to uphold and defend the Constitution and oppose the overthrow of the government by illegal means. Cole v. Richardson, 405 U.S. 676 (1972).

termination procedures to employees in nonsensitive positions while at the same time recognizing:

> There is an obvious justification for the summary suspension power where the employee occupies a "sensitive" position in which he could cause serious damage to the national security during the delay incident to an investigation and the preparation of charges. Likewise, there is a reasonable basis for the view that an agency head who must bear the responsibility for the protection of classified information committed to his custody should have the final say in deciding whether to repose his trust in an employee who has access to such information. 351 U.S. at 546.

Similarly, the Court in United States v. Robel, in striking down a provision that made it unlawful for a member of a Communist-action organization to be employed in any defense facility, noted that the prohibition sweeps all forms of membership and is not limited to sensitive positions in a defense facility. 389 U.S. at 266. Justice Brennan, concurring in the result in Robel semed to concede that "there may be 'defense facilities' so essential to our national security that Congress could constitutionally exclude all Party members from employment in them." Id. at 272. Finally, the cases invalidating loyalty oaths and associational inquiry have involved applicants for nonsensitive positions, a factor noted by the courts. Ozoroff, Stewart, Shapiro, Cummings, supra. See also, Law Students Research Council v. Wadmond, in which the Court upheld inquiry into organizational affiliations as a preliminary to further inquiry into the nature of the association, noting that "[s]urely a State is constitutionally entitled to make such an inquiry of an applicant for admission to a profession dedicated to the peaceful and reasoned settlement of disputes between men, and between a man and his government." 401 U.S. 154, 166 (1971).

Thus, a balancing test seems to have emerged with a wider leeway possibly being permitted in the investigation of applicants for employment in sensitive positions.

The compelling governmental interest in protecting the national security has also been recognized in cases upholding restrictions on employee activities in situations involving intelligence or national security. Snepp v. United States, 444 U.S. 507 (1980) (upholding CIA secrecy agreement); Haig v. Agee, 453 U.S. 280 (1981) (validating revocation of passport of CIA critic); McGehee v. Casey, 718 F. 2d 1137 (D.C. Cir. 1983) (upholding CIA classification and censorship program).

II

The Privacy Act of 1974, 5 U.S.C. 552a, is also cited as contributing to the demise of an effective federal loyalty security program.[4/] Critics point to sections (e)(6) and (e)(7) of the Act and the difficulty in protecting confidential sources of information under both the Privacy Act and the Freedom of Information Act (5 U.S.C. 552) as primary impediments.

The Privacy Act imposes requirements on federal agencies with respect to the collection, maintenance and dissemination of personally identifiable records. Subsection (e)(6) of the Act requires an agency to, "prior to disseminating any record about an individual to any person other than an agency..., make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes." Subsection (e)(5) contains a similar requirement with respect to records used in "making any determination about any individual." Subsection (e)(7) provides that an agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

[4/] See, Lewy, supra note 2 at 48-57; Martin, supra note 2 at 85.

Doubtless these and other provisions of the Privacy Act have imposed greater administrative burdens on agencies that collect and maintain background information on employees and applicants for employment. The provisions noted above, however, contain exceptions and have in some cases been interpreted by the courts in such a manner as to diminish their apparent stringency. For instance, the (e)(6) requirement that the record be accurate, relevant, timely and complete, is triggered only if the record is to be disseminated to a non-agency. Furthermore, both (e)(6) and (e)(5) require that the agency make only reasonable efforts to comply.

The (e)(7) prohibition on maintenance of records relating to the First Amendment activities of persons has also been construed to permit various record maintenance practices as being "pertinent to and within the scope of an authorized law enforcement activity." Thus, an investigation with respect to First Amendment activity is permissible under the Act if it is "relevant to an authorized criminal investigation or to an authorized intelligence or administrative one." Jabara v. Webster, 691 F. 2d 272, 279-80 (6th Cir. 1982). An employer's maintenance of records on employee job performance and data designed to prevent employee conflicts of interest have also been held to come within the law enforcement exception to (e)(7). Nagel v. Dept. of HEW, 725 F. 2d 1438 (D.C. Cir. 1984); American Federation of Govt. Employees v. Schlesinger, 443 F. Supp. 431, 435 (D.D.C. 1978). Thus, at least in the context of the employer - employee relationship, subsection (e)(7) would seem to permit a wide range of records maintenance by agencies.[5/]

[5/] The decision in Gang v. Civil Service Commission (1977), has been cited as representing the consequences that attach to agency maintenance of First Amendment records. See, Lewy, supra note 2 at 33-4; Letter from Alan Campbell, CSC Chairman, to Senator Thurmond, reprinted in Hearings on the Erosion of Law Enforcement Intelligence and Its Impact on the Public Security Before a Subcomm. of the Senate Judiciary

(continued)

There has been relatively little case law on the Privacy Act. The Act contains remedial limitations and numerous exceptions and provisos that make its enforcement by private litigants difficult.[6] Nevertheless, its provisions demand greater vigilance on the part of agencies in collecting, maintaining, and disseminating individually identifiable records.

It is also asserted that both the Privacy Act and the Freedom of Information Act (FOIA) have made sources of information fearful that confidential information supplied to government agencies is not secure. Both Acts on their face permit the withholding of information that could lead to the identification of confidential sources of information. 5 U.S.C. 552(b)(7); 552a(k)(5). The case law has also uniformly upheld use of these exemptions to protect confidential sources, both individual and institutional sources (such as state and local law enforcement agencies). Despite these safeguards, law enforcement agencies primarily have argued that the mere existence of the disclosure laws and the possibility of human error have created a perception on the part of would-be sources that information confided to the government may not be secure. It is this perception problem that has motivated some of the proposed amendments to the FOIA designed to place beyond the purview of the Act certain classes of records and strengthen existing exemptions in the law. See, S. Rept. 98-221, Freedom of Information Reform Act, 98th Cong., 1st Sess. 22-25 (1983). The very nature of the problem -- flowing as it does not from the actual

---

(continued) Comm. 95th Cong., 1st Sess. 232-3. The unreported case is reprinted at id., 233-6. However, later case law on (e)(7), supra, would seem to cast doubt on the Gang court's interpretation of that provision as prohibiting the maintenance of the type of employee security investigatory material at issue in the case. Of course, the relevance and timeliness fo the data in Gang was also at issue thereby implicating other provisions of the Act in addition to (e)(7).

[6] See, Litigation Trends Under the Privacy Act, reprinted in Hearings on Oversight of the Privacy Act Before a Subcomm. of House Government Operations Comm., 98th Cong., 1st Sess. 437 (1983).

operation of the law but from perceived dangers in the law — makes it difficult to ascribe particular problems in an information-gathering program such as a loyalty - security program to specific statutory provisions and recommend concrete remedies short of repeal of the Acts.

The decision in Doe v. United States Civil Service Commission, 483 F. Supp. 539 (S.D.N.Y. 1980) is also cited as damaging the loyalty - security program. There, an applicant (Doe) was denied a White House Fellowship because of derogatory information contained in a CSC background investigation report. The court held that the CSC unconstitutionally deprived Doe of a liberty interest by disclosing the derogatory information to the selecting agency without offering her an opportunity to rebut the charges. Such due process procedures are necessary, in the court's view, when a person is deprived of government employment and the alleged defamatory grounds are disclosed in a manner that forecloses other job opportunities. 483 F. Supp at 569. The court also indicated that in light of the rebuttal evidence offered by Doe, the CSC, if it refused to delete the derogatory information, must permit Doe to question the sources of the information.[7/] The court faulted the agency for not investigating the validity of the derogatory information despite substantial contrary evidence and not providing Doe an opportunity for rebuttal before placing the information in her file and disclosing it to another agency.

The precise deleterious impact, if any, on CSC procedures (and the ability to operate an effective loyalty - security program) posed by Doe is not entirely clear. The procedures of notice and hearing mandated by the court were apparently those normally followed by CSC in competitive service background investigations; they were not followed in this case of a non-competitive service position. See, 483 F.

[7/] The court did hold, however, that Doe could not obtain the names of the sources under the Privacy Act, citing 5 U.S.C. 552a(k)(5). 483 F. Supp. at 576.

Supp. at 573. The agency also modified its procedures as a result of Doe.[8] Furthermore, the Doe case itself was settled before revelation of the confidential sources became necessary and it has not appeared to spawn similar holdings. While the case holds out the possibility of compelled disclosure of confidential sources under some circumstances, the court itself noted that the cases would be "relatively infrequent..., where, because an allegation impugns a candidate's character so severely as to forclose future employment opportunities, due process requires notice and a chance to be heard." 483 F. Supp. at 573 n. 30. As with the Privacy Act and the FOIA, however, the perception of the problem posed by cases such as Doe may be more severe than any actual impact of the case itself.

III

The foregoing has been an overview of critics' charges regarding the impact of certain cases and statutes on the federal loyalty-security program. While the cases and privacy laws have necessitated refinements in the collection and maintenance of information on individuals and have likely increased administrative burdens, there seems to be agreement that they alone have not caused what is seen as the demise of the loyalty-security program nor can they be pointed to as making impossible a program geared to the legitimate needs of national security.[9] Other factors such as public aversion to certain information collection activities, the professionalism of those conducting background investigations and budgetary restraints have played a large role in the present state of the loyalty-security program.[10]

8/ See, Hearing on Government Files: Retention or Destruction Before a Subcomm. of Senate Judiciary Comm., 97th Cong., 1st Sess. 441 (1981).

9/ See, Lewy, supra note 2 at 42, 81-2; Committee Print, The Erosion of Law Enforcement Intelligence and Its Impact on the Public Security, supra note 2 at 131.

10/ Lewy, supra note 2 at chap. 5, 6; Martin, supra note 2 at 98, 124.

There is no doubt that judicial decisions and privacy legislation have made it more difficult to amass and disseminate data on the beliefs, associations and activities of individuals. Whether such data is necessary for an effective loyalty – security program and whether the current state of the program is an ineluctable result of such developments are issues that can be addressed in conjunction with an examination of the merits of the present state of case and statutory law.

Richard Ehlke
Richard Ehlke
Specialist in American
Public Law
American Law Division
November 2, 1984

EXHIBIT NO. 4

Congressional Research Service
The Library of Congress

Washington, D.C. 20540

February 8, 1985

TO : Senate Permanent Subcommittee on Investigations
Attention: Fred Asselin

FROM : Frederick M. Kaiser
Specialist in American National Government
Executive Branch Organization and Operations Section
Government Division

SUBJECT : Personnel Security Investigations for National Security and Intelligence Employees

This memorandum is in response to the Subcommittee's request for background information and analysis on security investigations of Federal personnel and private contractors involved in intelligence and national security matters and for a discussion of related oversight questions. If I may be of further assistance, please call me at 287-8682.

BACKGROUND

At present, four agencies conduct the overwhelming majority of all personnel security investigations for the Federal Government. 1/ They are: the Office of Security in the Central Intelligence Agency (CIA), the Defense Investigative Service (DIS) in the Department of Defense (DOD), the Federal Bureau of Investigation (FBI), and the Office of Personnel Management (OPM).

1/ U.S. Congress. House. Permanent Select Committee on Intelligence. Subcommittee on Oversight. Pre-Employment Security Procedures of the Intelligence Agencies. Hearings, 96th Cong., 1st Sess., May 16, 17, and 24 and June 21, 1979. Washington, U.S. Govt. Print. Off., 1980. passim.

Two other agencies 2/ authorized to conduct their own personnel security investigations are the Defense Department's National Security Agency (NSA) and the Department of State. NSA normally relies on security checks by the Defense Investigative Service but conducts its own special background investigations when there is an urgent need. The State Department conducts its own investigations of personnel with access to highly restricted Sensitive Compartmented Information (SCI). 3/

Recent Developments and Current Issues

The number of recent arrests and prosecutions for espionage, 4/ both in the United States and allied countries, have prompted considerable concern over the adequacy of existing procedures, measures, and practices designed to protect against unauthorized disclosures of classified national security information and intelligence products, sources, and methods. During the past

---

2/ Ibid., p. 2 and 57.

3/ SCI refers to highly restricted materials and information which are "classifiable" and available only to a separate and narrower category of employees among those with security clearances. SCI "involves or is derived from intelligence sources and methods and is classified or classifiable under the standards of Executive Order 12356 or under other Executive order or statute." This working definition is provided in the Sensitive Compartmented Information Nondisclosure Agreement, based upon National Security Decision Directive 84, Safeguarding National Security Information, March 11, 1983.

4/ Among other sources, see U.S. Congress. House. Permanent Select Committee on Intelligence. Report on Activities. House Report No. 98-1196, 98th Cong., 2d Sess. Washington, U.S. Govt. Print. Off., 1985, p. 12-14; U.S. Congress. Senate. Select Committee on Intelligence. Report. Senate Report No. 98-665, 98th Cong., 2d Sess. Washington, U.S. Govt. Print. Off., 1985, p. 37-39; New York Times, Jan. 13, 1985, p. 1, 20; and Washington Post, Jan. 12, 1985, p. A18, Jan. 9, 1985, p. A12, Jan 13, 1985, p. A11, Dec. 27, 1984, p. A3, Dec. 19, 1984, p. A18, Dec. 5, 1984, p. A18, Dec. 1, 1984, p. A3, Nov. 30, 1984, p. A14, Nov. 29, 1984, p. A22 and A42, Nov. 28, 1984, p. A4, Oct. 23, 1984, p. A12 and B2, Oct. 13, 1984, p. A4, Oct. 6, 1984, p. A3, Oct. 5, 1984, p. A1, A17, and Oct. 4, 1984, p. A1, A31.

year, arrests and prosecutions in the United States for illegal disclosures have included current or former employees of the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), for the first time in its 75-year history, the Army Intelligence and Security Command, and private contractors having access to classified information.

A separate reason for interest in this field has been President Reagan's National Security Decision Directive 84 (NSDD-84), issued March 11, 1983. It established new procedures for safeguarding national security information, including nondisclosure agreements affecting former employees. Of particular import here was that NSDD-84 authorized the expanded use of polygraph testing for Federal employees and private contractors having access to classified information. The Directive provides for the use of polygraphs as a condition of employment, as a condition of access to classified information, in criminal investigations, and in administrative investigations.

Because of the secrecy surrounding personnel security investigations, public knowledge about internal security operations, procedures, practices, and findings is sketchy at best. Nevertheless, when public concern is expressed about personnel security investigations, one or more of the following four questions are usually raised. (1) What degree of cooperation is there among agencies in conducting such investigations? (2) What are the civil liberties and rights of employees being investigated by the agencies? (3) What is the cost, effectiveness, and appropriateness of particular techniques and procedures in use? (4) What is the authority under which each agency operates and is it sufficient or overly vague? Each of these questions raises oversight issues which are discussed in this memorandum beginning on page 8.

Jurisdiction and Authority for Congressional Oversight

An initial consideration is whether congressional oversight jurisdiction for this subject is shared among several committees or held exclusively by the Select Committees on Intelligence in the House and Senate. Both Select Committees have consolidated oversight jurisdiction for the U.S. Intelligence Community and have already conducted inquiries into counterintelligence operations, foreign espionage activities, and personnel security investigations. 5/

Despite the inherent jurisdictional authority over such matters residing in the Senate with the Select Committee on Intelligence, it does not possess that responsibility exclusively. Intelligence oversight jurisdiction in the Senate is shared among several committees for two main reasons: because of the diversity of the issues and institutional locations of agencies involved, and because of the formal jurisdictions of various Senate standing committees and express restrictions on the Select Committee on Intelligence.

The resolution establishing the Senate Select Committee on Intelligence expressly recognizes "the authority of any other committee to study and review any intelligence activity to the extent that such activity directly affects a matter otherwise within the jurisdiction of such committee." 6/ It further adds:

> Nothing in this resolution shall be construed as amending, limiting, or otherwise changing the authority of any standing committee of the Senate to obtain full and prompt access to

---

5/ House Select Committee on Intelligence, Pre-Employment Security Procedures; U.S. Congress. Senate. Select Committee on Intelligence. Report. Senate Report No. 98-10, 98th Cong., 1st Sess. Washington, U.S. Govt. Print. Off., 1983. p. 13-16, 23-24, and 34; and Senate Select Committee Report 98-665, p. 24-27, 29-30, and 37-39.

6/ S. Res. 400, 98th Cong., 2d Sess.

> the product of the intelligence activities of any department or agency of the Government relevant to a matter otherwise within the jurisdiction of such committee. 7/

Other Senate committees with appropriate jurisdiction include Appropriations, Armed Services, Foreign Relations, and the Judiciary as well as Governmental Affairs, the Permanent Subcommittee on Investigations' parent committee. The Senate Governmental Affairs Committee possesses comprehensive oversight jurisdiction to study "the efficiency, economy, and effectiveness of all agencies and departments of the Government" 8/ and has held hearings on the Reagan Administration's initiative in personnel security, NSDD-84. 9/

Congressional oversight of the executive is a well-established and broad authority. 10/ Yet the sensitivity and secrecy surrounding certain aspects of personnel security investigations of national security and intelligence agencies place peculiar demands and constraints on the congressional oversight process. These include concerns for protecting individual rights and civil liberties, including the right of privacy, as well as for preserving the confidentiality of communications from the affected agencies where appropriate.

Congress has recognized the need to preserve the secrecy of certain matters for a variety of reasons. In so doing, Congress has protected governmental operations and activities which might otherwise be jeopardized and avoided

---

7/ Ibid.

8/ Paragraph 1(k)2 of Senate Rule 25.

9/ U.S. Congress. Senate. Committee on Governmental Affairs. National Security Decision Directive 84. Hearing, 98th Cong., 1st Sess., Sept. 13, 1983. Washington, U.S. Govt. Print. Off., 1983.

10/ The Supreme Court has legitimated that authority in Watkins v. United States, 354 U.S. 178, at 187 (1957) and in Barenblatt v. United States, 360 U.S. 109, at 111 (1959). A selective bibliography at the end of this memorandum cites studies of the congressional oversight in general and of the U.S. Intelligence Community in particular.

accusations of irresponsibility from the President and others, if such information is released prematurely or improperly. Congress has also entered into agreements with the Executive Branch to keep certain materials secure in order to acquire sensitive information and in recognition of the statutory obligation of the Director of Central Intelligence to protect "intelligence sources and methods from unauthorized disclosure." 11/ Such agreements have also been advanced to avoid Executive Privilege claims that might have resulted in a constitutional stalemate. Even if such a claim could be successfully challenged in Federal court (not a foregone conclusion in matters of national security), the process might result in a lengthy delay before Congress actually received the disputed information or documents. 12/

Illustrative of these features are several examples of congressional investigations and oversight arrangements. When the Oversight Subcommittee of the House Select Committee on Intelligence investigated pre-employment security procedures of the intelligence agencies in 1979, it granted an exception to agency officials testifying about on-going practices: The Subcommittee Chairman advised agency officials that "should any question come up" during the open session hearings "the answer to which is classified, the witnesses should inform the committee that a response would be given in executive session and we can deal with it in executive session." 13/

11/ P.L. 80-253; 61 Stat. 498.

12/ See, for instance, United States v. Nixon, 418 U.S. 683 (1974).

13/ House Intelligence Oversight Subcommittee, Pre-Employment Security Procedures, p. 1.

Beyond this, congressional committees have established exacting procedures to safeguard classified or sensitive information from unauthorized disclosures. 14/ Some protective measures and procedures, as those of the defunct Joint Committee on Atomic Energy and the current Select Committees on Intelligence, have been extremely elaborate and have been explicitly authorized by statute and Chamber rule. Despite the oversight authority and jurisdiction of other congressional committees, only the House and Senate Select Committees on Intelligence have an express statute and Chamber rules governing the acquisition of classified or sensitive information from the U.S. Intelligence Community. The Intelligence Authorization Act for FY 1981 15/ obligates the heads of intelligence agencies to keep the House and Senate Select Committees "fully and currently informed of all intelligence activities . . . including any significant anticipated activity" and orders those officials to "furnish any information or material concerning intelligence activities which is in" their possession. The same law, however, requires that the recipient select committees establish "procedures to protect from unauthorized disclosure all classified information and all information relating to intelligence sources and methods furnished to the intelligence committees." 16/ That provision echoes the separate responsibility of the Director of Central Intelligence for "protecting intelligence sources and methods from unauthorized disclosure." 17/

14/ For a survey of procedures adopted by congressional committees, see U.S. Library of Congress. Congressional Research Service. Congress and Procedures for Protecting Security or Intelligence Information. Report No. 79-105 GOV, by Harold Relyea. Washington, 1979; and U.S. Library of Congress. Congressional Research Service. Non-Committee Member Access to Information in the Custody of the House Permanent Select Committee on Intelligence. Typed report by Frederick M. Kaiser, Dec. 17, 1984.

15/ P.L. 96-450; 94 Stat. 1982.

16/ Ibid.

17/ P.L. 80-253; 61 Stat. 498.

In addition, congressional inquiries into personnel security investigations by intelligence and national security agencies must also be concerned with protecting the constitutional rights of individuals. Considerable damage might be done to careers and reputations by public revelations of improper, unethical, or illegal conduct based upon scanty evidence or unsubstantiated allegations. Recognizing this possibility, the Supreme Court had cautioned in both the Watkins and Barenblatt opinions, cited above, that Congress' investigative power was not unlimited. "There is no general authority to expose the private affairs of individuals without justification in terms of the functions of Congress," the Court held in Watkins. "Nor is the Congress a law enforcement or trial agency." 18/ "Congress, in common with all branches of the Government," Justice Harlan subsequently reasoned, "must exercise its powers subject to the limitations placed by the Constitution on governmental action, more particularly in the context of this case the relevant limitations of the Bill of Rights." 19/

OVERSIGHT ISSUES

Recent developments and expressions of public concern present four sets of oversight issues, which are discussed below.

--Interagency cooperation and coordination

--Civil liberties and rights of employees and contractors

--Cost, effectiveness, and appropriateness of investigative techniques

--Authority of agencies

18/ 354 U.S., at 187.

19/ 360 U.S., at 112.

Interagency Cooperation and Coordination

Because of the limited agency resources, the unusual expertise required in security investigations, and the interrelated responsibility of the agencies, the Subcommittee may be interested in examining cooperation and coordination among them. It might be asked in which areas, to what degree, and with what mechanisms and results, do the FBI, CIA, OPM, and DIS cooperate or share responsibility to ensure and maintain personnel security standards? What is being done cooperatively among these agencies, as well as with NSA and the Department of State, to prevent unauthorized disclosures of classified information by Federal personnel and private contractors?

Each agency or its parent department, of course, has its own statutory or administrative duties in these matters. Yet, it is uncertain (from an outside perspective) whether there are clear, well-established boundaries for such authority and whether adequate and appropriate mechanisms for coordination exist.

One area of potential concern centers on the possible conflict between the statutory mandate of the Director of Central Intelligence (DCI) to protect "intelligence sources and methods from unauthorized disclosure" versus the prohibition on the CIA against "police, subpoena, law-enforcement powers, or internal-security functions." 20/ It may still be possible, as in the

---

20/ P.L. 780-253; 61 Stat. 498.

past 21/ that confusion or legitimate differences of opinion can arise over the proper scope of the DCI's authority to protect sources and methods and the need to rely upon the FBI for police actions, law enforcement, and internal security.

The Director of Central Intelligence, in an administrative directive (DCID 1/14), has specified the eligibility requirements and minimum investigative standards for employees with access to Sensitive Compartmented Information. 22/ It is uncertain, however, what authority the DCI has to monitor and supervise implementation of these standards in other departments and agencies and to call for or mandate corrections of perceived deficiencies in such agencies.

In an attempt to improve coordination among national defense and intelligence agencies, several organizational changes have been made. In 1978, a small interagency counterintelligence staff, drawn from the FBI, CIA, and Defense Department and assigned to the DCI, was instituted to "make regular overall assessments of threats and U.S. countermeasures." 23/ Later, in 1982, "a Senior Interagency Group-Intelligence was established under the National

---

21/ For example, in the mid-1970s, the President's Commission on CIA Activities within the United States, commonly referred to as the Rockefeller Commission, reported on CIA surveillance of an employee who "had been privy to extremely sensitive classified information" and who "attended meetings of a group which the Agency suspected of foreign left-wing support." The CIA's surveillance extended to physical surveillance for nearly a year, a mail cover for seven months, electronic eavesdropping (via surreptitious entry), and a tax return review. U.S. President's Commission on CIA Activities within the United States. Final Report. Washington, U.S. Govt. Print. Off., 1975. p. 163-165.

22/ For a review of earlier compliance with this directive (DCID 1/14) among various intelligence agencies, see House Intelligence Oversight Subcommittee, Pre-Employment Security Procedures, passim.

23/ Senate Select Committee on Intelligence, 1983 Report, p. 23.

Security Council with two working interagency groups for counterintelligence and countermeasures." 24/ One question arising from these organizational changes is whether the new groupings directly or indirectly involve other related agencies, such as the Army Intelligence and Security Command or the Information Security Oversight Office? Others are: How frequently do the interagency groups meet and what specific measures have been advocated and implemented?

The Subcommittee might consider examining the CIA-FBI-DIS-OPM relationship to determine the following: What examples of cooperation and coordination exist, in addition to organizational changes? Have memoranda of understanding among the agencies been adopted to delineate each one's responsibilities and to initiate FBI investigations of Defense Department or CIA personnel and other agency personnel, contract employees, or outside contacts? Do any of the agencies consider the present arrangements inadequate or inappropriate; and if so, why?

Occasionally, accusations surface that a "mole" (a foreign intelligence agent or plant) has penetrated one of the intelligence agencies. In such cases, has the FBI been called in to investigate the CIA or Defense establishment? Investigation by the FBI, rather than by the agencies in question, could be justified on the grounds that the FBI would be a more objective and impartial investigator, might use different investigative techniques, and might be more experienced in such investigations. 25/

24/ Ibid.

25/ Allegations about Soviet penetration of the General Accounting Office (GAO) were publicized in 1981. Despite its own internal security arrangement and its position as a Legislative Branch entity, GAO was investigated by the FBI, which, incidentally, found no substantiation to the charges. Ibid., p. 34; and Congressional Record, v. 128, Sept. 24, 1982. p. S12286-S12287.

In 1979 hearings on pre-employment clearances, executive branch officials identified the Security Committee under the Director of Central Intelligence as the primary coordinative mechanism. 26/ Does it still exist and serve that role? To what extent do present officials and field operatives in the three agencies regularly compare and discuss their findings, methods, and procedures for maintaining personnel security? Do the methods and procedures differ among these agencies and if so why?

Additional questions about the level and extent of interagency cooperation are suggested by President Reagan's Executive Order 12333 of December 4, 1981. Under this Order each agency within the U.S. Intelligence Community, under procedures approved by the Attorney General, is empowered to collect, retain, or disseminate information that constitutes foreign intelligence and counterintelligence, that protects foreign intelligence or counterintelligence sources or methods from unauthorized disclosure, and that concerns persons who are believed to be potential sources or contacts for the purpose of determining their suitability or credibility. 27/ This information has obvious significance for the presonnel security offices of the FBI, CIA, OPM and DIS.

Have such procedures been established in compliance with the Executive order's directive? Since such information may be disseminated to the other security agencies, does that occur on a regular basis through an established process? Has this information proven to be reliable and what types of standards, if any, have been erected to ensure its reliability? Moreover,

---

26/ House Intelligence Oversight Subcommittee, Pre-Employment Security Procedures, p. 12.

27/ Federal Register, v. 46, Dec. 8, 1981. p. 59950.

what use is made of the information that is disseminated to other agencies and how much of it is retained by the recipient? 28/

To assist in this oversight process, the Subcommittee might request that the General Accounting Office (GAO) evaluate the information-gathering and dissemination practices under E.O 12333. This would be similar to GAO's reviews of FBI domestic intelligence operations conducted in the mid- and late-1970s, the first GAO examinations of the FBI in its then nearly seventy-year history. 29/ Since then, incidentally, GAO has established an on-site audit capability at the FBI and has conducted other examinations of confidential operations. 30/ However, GAO has yet to re-establish an audit and investigative capibility over the CIA.

28/ Under E.O. 12333, the receiving agency determines whether it will retain the information provided by another agency. But unless such information is highly regarded and reliable, it may prove to be as burdensome as useful to the recipient. In an earlier case where information lacked reliability or was perceived as inappropriate, for example, most of the transmitted intelligence was discarded. U.S. General Accounting Office. FBI Domestic Intelligence Operations—Their Purpose and Scope: Issues That Need to be Resolved. GGD-76-50, Feb. 24, 1976. Washington, 1976. p. 125. That finding, in turn, led to a directive from Attorney General Edward H. Levi, changing the existing arrangements. U.S. Attorney General. Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest. Washington, Mar. 10, 1976. p. 3, Part III. A.

29/ GAO, FBI Domestic Intelligence Operations, 1976. GAO also issued a followup report to its 1976 study. U.S. General Accounting Office. FBI Domestic Intelligence Operations: An Uncertain Future. GGD-78-10, Nov. 9, 1977. Washington, 1977.

30/ See, for instance, U.S. General Accounting Office. FBI-DEA Task Forces: An Unsuccessful Attempt at Joint Operations. GGD-82-50, Mar. 26, 1982. Washington, 1982.

Civil Liberties and Rights of Employees and Contractors

Related to concerns for reliability are interests in safeguarding the rights of agency employees and contractors, who might be slandered or libeled in such information-gathering enterprises or who might even be unaware of allegations made against them. The possibility of misinformation or inaccuracies in these security files and abuse of the information-gathering process is greater in personnel security matters than in criminal investigations. (In the latter, information used in prosecutions must meet certain court-imposed standards for admissibility and may be subject to cross-examination.) In the former, the information may not be used in court proceedings, exposed publicly, or even made fully available to the individual in question, thereby precluding full personal, public, judicial, or other governmental agency scrutiny.

The principal reasons for this situation are the discretionary exemptions to information access laws. The Freedom of Information Act (FOIA) and Privacy Act contain certain specific exemptions that severely restrict access to personnel security files and thus make it difficult to evaluate their use, accuracy, and reliability. 31/

The 1984 Amendments to FOIA extended specific exemptions for the CIA to specified operational files. 32/ Those are the files of the Directorate

---

31/ 5 U.S.C. 552, and 552 a(j) and (k)(5) (1982). For a congressional review of FOIA, see U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure. Agency Implementation of the 1974 Amendments to the Freedom of Information Act; Report on Oversight Hearings. Committee Print. 95th Cong., 2d Sess. Washington, U.S. Govt. Print. Off., 1980.

32/ P. L. 98-447; 98 Stat. 2209.

of Operations which document the conduct of counterintelligence operations and security liaison arrangements or information exchanges with foreign governments or their intelligence or security services, and the files of the Office of Security which document investigations conducted to determine the suitability of potential foreign or counterintelligence sources. A second provision of the 1984 Amendments notes that such exempted operational files shall continue to be subject to search and review for information for specific investigations. It expressly identifies, however, the "intelligence committees of the Congress" and no other Congressional office among the governmental entities eligible to search them automatically.

The Senate Intelligence Committee reported in 1983 that it had sought to determine "whether there are adequate safeguards to prevent misuse" of the counterintelligence investigative authority in E.O. 12333 but did not elaborate upon its findings. 33/ The Permanent Subcommittee on Investigations might consider examining such procedures on its own, not only to protect the rights of U.S. citizens and others but also to ensure a tighter, more reliable intelligence product. The same concerns—for accuracy, reliability, and individual rights—might be applied to the personnel-security agencies' use of State and local criminal history files. This is especially important since the guidelines of States and localities vary and do not necessarily meet Federal agency standards for their own collections. 34/ The Subcommittee might also consult

---

33/ Senate Select Committee on Intelligence, 1983 Report, p. 24. Related concerns for protecting employee rights in internal investigations have existed in other sensitive, confidential areas, such as police organizations. See John H. Burpo. The Policeman's Bill of Rights. The Police Chief, Sept. 1972. p. 18-19; and U.S. National Advisory Commission on Criminal Justice Standards and Goals. Police. Washington, U.S. Govt. Print. Off., 1973. p. 469-495.

34/ For a description, see an article by the DIS Deputy Director for Industrial Security. Daniel J. Dinan. Defense Investigative Service: Access to Criminal Hisotry Records. The Police Chief, v. 50, Feb. 1983. p. 20-21.

GAO, which has had experience examining FBI responses to FOIA and Privacy Act requests and might be in a position to assist in an evaluation of the personnel files. 35/

Cost, Effectiveness and Appropriateness of Techniques

The FBI, CIA, OPM, and DIS have a variety of investigative techniques available for initiating and maintaining security clearances for Federal personnel and contractors. Collectively, they cover a wide range of devices: mail covers, mail openings, background security checks, electronic surveillance, physical surveillance, polygraph testing, and even "scams." They vary in their use, appropriateness, and intrusiveness as well as in costs and effectiveness.

Because of the absence of authoritative, comprehensive data on their present use, however, the Subcommittee, at the outset of its oversight examination, would need to discover what techniques are used by each agency, for each type and level of security clearance. It would also be useful to know how allegations of suspicious conduct are handled at different stages of the (prospective) employee's or contractor's career. If this data can be obtained, a comparison of agency personnel-investigations would be possible. This data could then lead to further questions about their differences and reasons for employing different techniques for similar problems or concerns. Following are some suggestions specific to two individual techniques, polygraphs and scams.

35/ U.S. General Accounting Office. Timeliness and Completeness of FBI Responses to Requests Under Freedom of Information and Privacy Acts Have Improved. GGD-78-51, April 10, 1978. Washington, 1978; and Impact of the Freedom of Information and Privacy Acts on Law Enforcement Agencies. GGD-78-108, Nov. 15, 1978. Washington, 1978.

The Reagan Administration has placed new emphasis on polygraph testing to protect against the unlawful disclosure of classified information. Based upon recommendations from an interdepartmental group convened by the Attorney General, President Reagan issued National Security Decision Directive 84 (NSDD-84). This Directive permits expanded use of polygraph examinations and institutes new enforcement mechanisms, including the prospect that "adverse consequences will follow an employee's refusal to cooperate with a polygraph examination." 36/ Yet, because of questions about the utility and reliability of polygraph testing for investigatory purposes, Congress approved a moratorium, which has since expired, on implementation of Department of Defense (DOD) guidelines which allow for expanded polygraph examinations. 37/

According to Administration testimony, the CIA and NSA employees periodically undergo polygraph testing. 38/ Moreover, the policies of the Justice Department,

---

36/ U.S. President, 1981- (Reagan). Presidential Directive on Safeguarding National Security Information. March 11, 1983. For a description of the process leading to NSDD-84 and a defense of the Administration's position, see the statement by Deputy Assistant Attorney General Willard, who headed the interagency committee upon whose recommendations the Directive is based. In U.S. Congress. House. Committee on Government Operations, Subcommittee on Legislation and National Security. Review of the President's National Security Decision Directive 84. Hearings, 98th Cong., 1st sess., Oct. 19, 1983. Washington, U.S. Govt. Print. Off., 1984. p. 169-218.

37/ This is found in DOD's FY 1984 Authorization Act (P.L. 98-94). For a discussion of the moratorium and congressional objections to the new DOD guidelines, see Congressional Record, Daily Edition, v. 129, July 15, 1983. p. S1044-S1048. Subsequently bills have been introduced to make the temporary prohibition permanent: H.R. 4681 in the 98th Congress and H.R. 39 in the 99th Congress. Of related interest is the Office of Technology Assessment's 1983 study of polygraph examinations. U.S. Office of Technology Assessment. Scientific Validity of Polygraph Testing: A Review and Evaluation. Washington, 1983.

38/ Willard, Safeguarding National Security Information, p. 178.

as well as the CIA and NSA, "already satisfy the requirements of NSDD-84" and OPM "has clarified its policies as being consistent with NSDD-84." 39/ Do such examinations lead to followup investigations, and, presumably in conjunction with other investigative techniques, to dismissals or transfers of personnel? What types of followup inquiries or investigations commence after polygraph testing that may be inconclusive or that suggest suspicious behavior by the subject? How frequently do personnel undergo polygraph testing and do successive tests differ?

A second controversial investigative technique, which may be used in continuing personnel security investigations, is the "scam," whereby a government investigator or informant poses as a middleman in a false criminal conspiracy in order to obtain incriminating evidence (frequently tape-recorded or videotaped) against an individual. 40/ The fundamental questions are whether the scam is an appropriate investigative tool in such cases and whether it is used with any frequency in determining the security status of Federal personnel and contractors. Evidence of espionage in two recent cases involving a former

---

39/ Ibid.

40/ Publicized most recently in ABSCAM, Brilab, and the De Lorean prosecutions, scams have been most closely associated with white collar crime and political corruption investigations. For a review of the composition, issues, and controversies surrounding scams, see U.S. Congress. House. Committee on the Judiciary. Subcommittee on Civil and Constitutional Rights. FBI Undercover Operations. Report of the Subcommittee. Committee Print, 98th Cong., 2d Sess. Washington, U.S. Govt. Print. Off., 1984; U.S. Congress. Senate. Select Committee To Study Undercover Activities of Components of the Department of Justice. Final Report. Senate Report no. 97-682, 97th Cong., 2d Sess. Washington, U.S. Govt. Print. Off., 1982; and Gerald M. Caplan, (ed.). ABSCAM Ethics: Moral Issues and Deception in Law Enforcemnt. Washington, The Police Foundation, 1983.

counterintelligence officer with the Army Intelligence and Security Command and a private contractor attempting to sell national defense secrets appears to have been obtained through scams. 41/

The argument could be made that the scam technique, at least on a selective basis, would be a useful counterespionage device, because individuals involved in national security and intelligence matters possess valuable information for which there exists an established, acquisitive, and credible market. The constitutionality and legality of some scams have been upheld by Federal courts in criminal prosecutions, as long as entrapment does not occur. Thus, their use for internal agency security and counterespionage could be defended as a means of identifying Federal employees and contractors (with access to classified or sensitive information) who might be bribed or compromised, without actually risking the loss of that classified information to a foreign agent. Of course, there are serious objections to scams, based upon practical problems of cost, control, and accountability. Also, legitimate concerns exist about the ethics of using a technique that fosters criminal conduct or a breach of security, that compromises or incriminates an individual who may not have committed any previous offense, and that may place the Government in the role of *agent provocateur*.

Do any of the personnel-investigative services use scams to identify or reveal suspected "turned" agents, presuming that other incriminating evidence

---

41/ Washington Post, April 11, 1984, p. 28, and Dec. 19, 1984, p. A18. Scams in related areas have occurred when convicted former CIA agent Edwin P. Wilson attempted to arrange for the assassination of two Washington prosecutors, among others, through an FBI agent posing as a hired killer. Washington Post, Feb. 6, 1983, p. A1 and A8, and Feb. 17, 1983, p. A31; and in 1979, when a Drug Enforcement Administration supervisor purportedly accepted bribes from an informer. New York Times, April 30, 1979, p. A11.

is unavailable? Has the scam technique been considered by any of the agencies as a means of deterring agents from potential espionage activities? If scams are part of the investigative repertoire, what guidelines and standards govern their use, what costs have accrued, what inducements (bribes, payoffs, compromising situations) are used, and what results have occurred?

In addition to the previous questions about techniques are their costs. Questions about costs, budgets, and resources might be considered from three different perspectives. 42/ One approach would compare costs to the workload of each of the units, to determine whether budgets and resources have kept pace with the quantity and quality of investigative methods. A second approach would assess costs and benefits of particular techniques, ascertaining how they compare with one another or over time. And a third would determine what savings or cost-avoidances might accrue from different techniques or approaches, from clarified standards, guidelines, and controls, and from improved coordination of the agencies.

Authority of Agencies

A final area of consideration is the adequacy of existing authority to maintain security and conduct personnel security investigations. Three basic

---

42/ Examples of different approaches appear in recent GAO examinations about personnel-security investigations and related matters; see U.S. General Accounting Office. Costs of FBI Undercover Operations. GGD-83-51, March 7, 1983. Washington, 1983; FBI Audit Conclusions on the Criminal Informant Program Should Have Been Qualified. GGD-80-37, March 13, 1980. Washington, 1980; Costs of Federal Personnel Security Infestigations Could and Should Be Cut. FPCD-79-79, Aug. 31, 1979; Faster Processing of DOD Personnel Security Clearances Could Avoid Millions in Losses. GGD-81-105, Sept. 15, 1981. Washington, 1981; and The Department of Justice Needs To Address the Problem of Two Personnel Investigations Being Conducted on All Bureau of Prison Employees. GGD-82-56, July 8, 1982. Washington, 1982.

questions in this regard immediately arise. Is that authority sufficient to mount investigations, without abridging the constitutional rights of personnel? Is official responsibility for such investigations and suspected breaches of security clarified? Is additional or different authority needed to ensure the proper performance of such duties?

Agency heads already hold impressive authority over their employees, derived from statute, executive order, and presidential directive. All positions in the CIA and FBI, as well as the National Security Agency (NSA), are statutory exceptions to the competitive service. This means that the agencies are exempted from civil service laws governing the selection, promotion, and removal of personnel. 43/ Epitomizing this broad discretionary authority is that granted to the Director of Central Intelligence, 44/ who is empowered to "terminate the employment of any officer or employee of the Agency whenever he shall deem such termination necessary or advisable in the

---

43/ See U.S. Congress. Senate. Committee on Post Office and Civil Service. Statutory Exceptions to the Competitive Service: A Report by the U.S. Civil Service Commission. Committee print, 93d Cong., 1st Sess. Washington, U.S. Govt. Print. Off., 1973. passim. In a recent case, for example, the FBI refused to hire an apparently well-qualified applicant (who had held a "secret" level clearance while with the Immigration and Naturalization Service). A Federal court sustained the FBI's authority and decision, although the Court did not reveal the specific reason because of a concern for harming national security if it did so. Molerio v. FBI, et al., 83-2095. See also Federal Times, v. 20, Dec. 17, 1984, p. 6.

44/ P.L. 80-253; 61 Stat. 498. Such authority, although unreviewable and incontrovertible within the Executive Branch, may still be subject to judicial review and constitutional constraints. A recent press account, for example, cites a Federal District Court judge's determination that the CIA had exceeded its authority by firing an employee on national security grounds after the employee acknowledged participating in homosexual activities. Washington Post, Jan. 18, 1985, p. A8. If sustained on appeal, this decision would overturn CIA policy of considering homosexuality, described in testimony in 1979, as "a risk, and a risk which has to be resolved in favor of the agency." Quote by the Director, CIA Office of Security, in House Intelligence Oversight Subcommittee, Pre-Employment Security Procedures, p. 47.

interest of the United States . . . " As noted above, E.O. 12333 allows intelligence agencies to exchange personnel-security and counterintelligence information. And NSDD-84 clarifies (in effect, supplements) "FBI authority to investigate cases in which administrative sanctions may be sought instead of criminal prosecution." 45/ Also the Defense Department may implement NSDD-84's provisions for polygraph testing whenever the Administration decides to do so. Such testing can be halted only by the passage of new legislation.

Several important concerns, however, still prompt consideration or investigation. In light of recent Federal court decisions, is there a need to further clarify agency authority over personnel. Contrariwise, is there a need to reduce or circumscribe it in certain areas, as with polygraph testing? Another idea has been to consolidate personnel investigative authority under the DCI, rather than having it dispersed among six different agencies. What are the benefits and liabilities of this proposal, especially in terms of standardization, costs, responsiveness, and concentrated authority?

45/ See statement by Deputy Assistant Attorney General Williard, in House Subcommittee on Legislation and National Security, Review of NSDD-84, p. 177.

SELECTIVE BIBLIOGRAPHY ON CONGRESSIONAL OVERSIGHT IN GENERAL AND OF THE INTELLIGENCE COMMUNITY

Aberbach, Joel. Changes in congressional oversight. American Behavioral Scientist, v. 22, 1979.

Crabb, Cecil and Pat Holt. Invitation to struggle: Congress, the President, and foreign policy. Washington, Congressional Quarterly Press, 1980, Chapter 6.

Elliff, John T. The legal framework for intelligence activities. Paper presented at the 80th annual meeting of the American Political Science Association, Washington, 1984.

English, Glenn. Congressional oversight of security classification policy. Government information quarterly, v. 1, 1984.

Franck, Thomas and Edward Weisband. Foreign policy by Congress. New York, Oxford University Press, 1979, Chapter 5.

Glennon, Michael. Investigating intellligence activities The process of getting information for Congress. In Thomas Franck, ed. The tethered Presidency. New York, New York University Press, 1981.

Godson, Roy. Congress and foreign intelligence. In Ernest Lefever and Roy Godson, eds. The CIA and the American ethic. Washington, Georgetown University, 1979.

Goldwater, Barry. Congress and intelligence oversight. The Washington quarterly, v. 6, Summer 1983.

Hamilton, James. The power to probe. New York, Vintage Books, 1976.

Johnson, Lock. The U.S. Congress and the CIA. Legislative studies quarterly, v. 5, 1980.

Kaiser, Fred M. Congressional oversight of foreign policy. Legislative studies quarterly, v. 2, 1977.

Karalekas, Anne. Intelligence oversight: has anything changed? The Washington quarterly, v. 6, Summer 1983.

Latimer, Thomas. U.S. intelligence and the Congress. Strategic review, v. 7, 1979.

Milberg, Warren. The role of Congress in the intelligence evaluation process. In Robert Pfaltzgraff, Uri Ra'anan, and Warren Milberg, eds. Intelligence policy and national security. Hamden, Conn., Archon Books, 1981.

Ogul, Morris. Congress oversees the bureaucracy. Pittsburgh, University of Pittsburgh Press, 1976.

Ransom, Harry Howe. CIA accountability: Congress as tempermental watchdog. Paper presented at the 80th annual meeting of the American Political Science Association, Washington, 1984.

U.S. Library of Congress. Congressional Research Service. Congressional oversight manual. Washington, 1984.

FK/dl/sam

EXHIBIT NO. 5

MEMORANDUM

June 10, 1985

TO: File

FROM: Fred Asselin
Investigator

RE: NATO

The following descriptions of personnel security policies and procedures of several NATO allies and France were prepared at the Subcommittee's request by various law sections of the Library of Congress.

FA/kd

PERSONNEL SECURITY IN THE FEDERAL REPUBLIC OF GERMANY

by Dr. Edith Palmer

Law Library
Library of Congress
April 1985

CONTENTS

List of Abbreviations i
I. Introduction 1
II. The Incidence of Espionage 1
III. The Political Parties 3
  A. General 3
  B. The Communist Party 4
  C. The Green Party 5
IV. Procedures in Personnel Security Investigations 7
V. Due Process in Security Investigations 10
VI. The Role of the Intelligence Agencies 11
  A. General 11
  B. The Offices for the Protection of the Constitution... 12
  C. The Military Defense Service 14
  D. The Federal Intelligence Service (BND) 15
VII. Restrictions on Interagency Cooperation 15
VIII. The Impact of Data Protection 15
IX. The Loyalty of Civil Servants 17
X. Comparison with Other West-European Countries 24
XI. Conclusion 25

LIST OF ABBREVIATIONS

BBG, Bundesbeamtengesetz, Federal Civil Service Law
BDSG, Bundesdatenschutzgesetz, Federal Data Protection Law
BfV, Bundesamt für Verfassungsschutz, Federal Constitution Protection Office
BGBl, Bundesgesetzblatt, official law gazette for the Federal Republic of Germany
BGS, Bundesgrenzschutz, Federal Border Protection Service
BND, Bundesnachrichtendienst, Federal Intelligence Service
BT, Bundestag, Federal Diet

DKP, Deutsche Kommunistische Partei, German Communist Party (since 1968)
DOV, Die Öffentliche Verwaltung
DVBl, Deutsches Verwaltungsblatt

EuGRZ, Europäische Grundrechte Zeitschrift

FAZ, Frankfurter Allgemeine Zeitung
F. Supp., Federal Supplement

IPOL, Polizeiliches Informations- und Auskunftssystem, Police Information System

KGB, Committee for State Security (Soviet Union)
KPD, Kommunistische Partei Deutschlands, German Communist Party (until 1956)

MAD, Militärischer Abschirmdienst, Military Defense Service

NADIS, Nachrichtendienstliches Informationssystem, Intelligence Information Service
NATO, North Atlantic Treaty Organization

RiA, Recht im Amt

SED, Sozialistische Einheitspartei Deutschlands, Socialist Unity Party (German Democratic Party)
SPD, Sozialdemokratische Partei Deutschlands, Social Democratic Party of Germany

TB, Tätigkeitsbericht des Bundesschutzbeauftragten, Annual Report of the Federal Data Protection Official

U.S., United States Supreme Court Reports

VuR, Verfassungsschutz und Rechtsstaat (Köln, 1981)

ZBR, Zeitschrift für Beamtenrecht
ZRP, Zeitschrift für Rechtspolitik

PERSONNEL SECURITY IN THE FEDERAL REPUBLIC OF GERMANY

I. Introduction

In the Federal Republic of Germany, personnel security in the Government is both an internal policy and a NATO obligation. This goal is pursued by various means that are based on many different laws and administrative practices. As is the case in the United States, the Federal Republic has also experienced a great deal of controversy in the implementation of its personnel security programs, and the problems in this field have been generated by the inherent tensions between national security and civil liberties. In the Federal Republic, as in the United States, the debate on this issue has been emotional, and it has been pursued with great intensity. The Government has been largely on the defensive and its practices have been questioned in the media, in the legal and political literature, in the courts and by legislative means. Altogether, these issues are far from being resolved, and they continue to excite public opinion.

A study of the legal framework for the German personnel security system and its problems may be of interest for various reasons, among them the possibility of gaining a better insight into our own problems in the United States. Despite the many differences between the legal and political systems in both countries, there are enough similarities in the personnel security problems encountered to make a closer look at the German situation worthwhile.

One of these similarities is the degree of discord that the personnel security issue has aroused in both countries, while other Western democracies have managed to deal with personnel security in less contentious ways. Other striking similarities are the attacks on a loyalty requirement for civil servants largely on the grounds of freedom of speech and assembly as well as the inroads made into the investigative methods of government by the impact of privacy legislation. Noteworthy among the differences between the two countries is the German insistence on official secrecy in contrast to the American concept of freedom of information, and the broader leeway given to the German Government to handle its affairs by internal, unpublished directives. These are just a few of the obvious aspects that invite comparison. Given the enormous amount of literature that the topic of national security versus civil liberties has created, its comparative evaluation might be a never ending story.

Instead, this report will look at some factors that determine the need for personnel security in the Federal Republic. Then an attempt will be made to piece together the actual investigative procedures from the few available sources that describe them. In addition, the participating intelligence services will be described together with the legal developments that threaten to impair their effectiveness by restricting their access to information. Also, the development of the loyalty requirement for civil servants will be summarized because it is in itself a measure of personnel security.

II. The Incidence of Espionage

Since its creation in 1949, the Federal Republic has been a prime target for espionage by the East Bloc countries. During the period 1953-1970, the West German authorities obtained information on 33,000 attempts by

East Bloc agents to recruit West Germans. [1] During the 1970s -- a decade characterized by detente and resulting in treaties between West Germany on the one hand and East Germany and Poland on the other -- the East Bloc even increased its espionage activities in Germany.

Since 1970, close to 40 persons per year have been convicted in West Germany for crimes of espionage. Among these was the famous case of Günter Guillaume, an East German spy who entered West Germany under the guise of a refugee and worked his way into a position of trust in the Federal Chancellery in Bonn where his role was discovered in 1974 in a scandal that led to the resignation of Chancellor Willy Brandt. Other notorious cases of that period involved West Germany military personnel and several unmarried female secretaries and typists employed by West German federal agencies. All these persons were recruited by East Germans, and their motives for becoming spies were money, romance, and ideology. [2]

A recent case of serious implications is the industrial espionage case of N. Rotsch who was discovered in the fall of 1984 as having passed important data on a major German weapons system to the Committee for State Security, KGB. Rotsch was an executive and engineer with the German firm Messerschmidt-Bökow-Blohm, the producer of the Tornado fighter plane. Rotsch emigrated from East Germany in 1954 at the age of 30 and worked for the Soviet secret service since 1967. [3]

Between 70% and 80% of the espionage in the Federal Republic is carried out by East Germany, the remainder by the other East Bloc countries. The East German Secret Service has a huge apparatus with special departments that focus on the penetration of the West German bureaucracy, the military, and the political parties. The East Germans have many obvious advantages for espionage in West Germany, notably the common culture, language, family bonds, etc. [4] In addition, East German refugees enjoy full citizenship status in the Federal Republic, including eligibility for civil service. [5] Yet, the granting of West German citizenship to East Germans, legally construed as one joint citizenship for all Germans, is an essential principle of the West German Constitution, and one that is emotionally and politically tied to the long-term goal of reunification. 6/

---

[1] E. Borer, Spionage 46 (Kreuzlingen, 1975).

[2] K. Fricke, "Spionage gegen die Bundesrepublik Deutschland," in Verfassungsschutz und Rechtsstaat [hereafter: VuR] at 297 (Köln, 1981).

[3] Frankfurter Allgemeine Zeitung [hereafter: FAZ] November 30, 1984, p. 3.

[4] Supra note 2.

[5] Arts. 16, 33, and 116, Grundgesetz für die Bundesrepublik Deutschland [hereafter: GG] vom 23. Mai 1949, Bundesgesetzblatt [BGBl, official law gazette of the Federal Republic of Germany] p. 1, as amended.

III. The Political Spectrum

A. General

West Germany's political system is dominated by a few stable, mainstream parties of proven democratic intentions. In addition, there are some splinter parties that have remained insignificant. Two fringe parties, however, merit a closer examination in terms of their potential to endanger German internal or external security. The Communists, who are not represented in the government except in a few local communities, nevertheless have shown considerable agility in all sorts of activities that are advantageous to their masterminds in the East Bloc. The Green movement, on the other hand, is a conglomerate of environmentalists, peace protesters, and various other single-issue groups, all held together by a dislike and distrust of established politicians. This political party has probably been used or infiltrated by the Communists, and the Greens have some potential for interfering with the country's security.

Among the extremists on the right and left, the terrorist Red Army Fraction should be mentioned in this context. Led by a small group of fanatics, they have attracted varying numbers of supporters over the past 15 years. The spectacular crimes committed by the terrorists and the antiterrorist measures employed by the government have attracted world-wide attention. 7/ Since 1972, it has been repeatedly suggested that terrorism has subsided, only for it to flare up again. 8/ As of January 1985, the police authorities again reported an increased strength among the terrorists who are now directing their efforts against military installations, including those of the U.S. 9/

6/ B. Schmidt-Bleibtreu and F. Klein, Kommentar zum Grundgesetz 1234 (Neuwied, 1983).

7/ M. Radvanyi, Anti-terrorist Legislation in the Federal Republic of Germany (Library of Congress, 1979).

8/ D. Conradt, The German Polity 80 (New York, 1982).

9/ FAZ, January 22, 1985, p. 4.

B. The Communist Party

The Communist Party (Kommunistische Partei Deutschlands, KPD) has not been represented in the federal government since 1953. In 1956 it was declared anticonstitutional by the Constitutional Court. [10] After this banishment and dissolution, the party led a shadow existence in various splinter groups within the Social Democratic Party (Sozialdemokratische Partei Deutschlands, SPD) or on its left fringe. [11] In 1968, the Communists reemerged as a political party under a slightly changed name (Deutsche Kommunistiksche Partei, DKP) and with a party program that pays lip service to the values of the Constitution and professes to seek alliances with other "antimonopolist forces in the Federal Republic." [12] By this, they mean an "alliance between communists, social democrats, trade unions, and Christian and non-party affiliated workers." [13]

The true allegiance of the DKP, however, lies with the party rulers in the Soviet Union and East Germany. Subservience to the East German party (Sozialistische Einheitspartei Deutschlands, SED) is particularly obvious: the DKP receives most of its financial support as well as regular instructions from the SED leadership. [14] The new party's democratic orientation is also a sham, and the party leaders reveal their true intentions in numerous written and oral pronouncements. In fact, the alliance with other democratic forces is merely a temporary strategy, preparatory to a seizing of power by violent means, which is to be followed by the establishment of a totalitarian regime. [15]

---

[10] Bundesverfassungsgericht [BVerfG] decision of 15. August 1956, 5 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 85 (1956).

[11] N. Johnson, State and Government in the Federal Republic of Germany 37 (Oxford, 1983).

[12] O. Model and C. Creifield, Staatsbürger-Taschenbuch 46 (München, 1983).

[13] Verfassungsschutz '72, at 66 (Bonn, 1973).

[14] Verfassungsschutz '79, at 89 (Bonn, 1980).

[15] P. Meier-Bergfeld, "Die Bündnispolitik der Deutschen Kommunistischen Partei," VuR, at 255.

These facts are well-known to the West German Government which keeps the Communist Party and its various affiliates and their activities under close observation. However, this new Communist Party has not been prohibited by the Constitutional Court. The initiation for such a proceeding lies at the discretion of the Government. In fact, such a proceeding has only been carried out twice since the creation of the Constitution. The other such incident was the outlawing of a fascist party in 1952. Since the reemergence of the Communist Party, the Government has preferred political contest to judicial action, and the Government can well afford this course of action since the membership in this party is stagnating at about 50,000, and the DKP has not achieved representation in either the Federal or a land parliament. 16/

Despite its low voter appeal, the Communist Party has been able to influence public opinion through various leftist groups under its control and through the infiltration of other groups such as the young socialists, several trade unions, and various political action committees on individual issues. 17/

One example of the Communists' effectiveness has been their work against the government's loyalty program. German law provides that civil servants must profess their loyalty to the Constitution by their entire conduct, and the German courts of last resort have repeatedly held that membership in the Communist Party or active participation in one of its front organizations is an act of disloyalty (*see* below). The Communist campaign to discredit this program has found mass support among Social Democrats and has succeeded in radicalizing public opinion on this issue. The Communist strategies on this issue have been very clever. By the creation of catchy slogans and allegations of fascist tendencies in the German bureaucracy, by the creation of numerous action groups, including some in other West European countries and the United States, an intense emotional climate has been created that is responsible for some of the modifications in the loyalty program that may have weakened it. 18/

C. The Green Party

Since 1980, the Green Party has been gaining representation in the parliaments of several *länder* (constituent states of the Federal Republic). In 1981, respectively 1982, the Green Party became a participant in the land governments of Hamburg and Hesse as the smaller coalition partner of the Social Democrats. In both these *länder*, the Green Party stands politically far to the left of the Social Democrats. Finally, in the March 1983 national parliamentary elections, the Greens won 5.6% of the vote, and since then they have been represented in the Federal Diet (*Bundestag*, representative chamber of the Federal bicameral legislature) with 27 seats. 19/

16/ K. von Beyme, *The Political System of the Federal Republic of Germany* 185 (Aldershot, 1983).

17/ *Supra* note 15, at 282.

18/ *Id.*; *Verfassungsschutz '81*, at 83 (Bonn, 1982).

19/ An excellent evaluation of the Green Party, its origins, goals and future is R. Pfaltzgraff, *et al.*, *The Greens of West Germany: Origins, Strategies, and Transatlantic Implications* (Cambridge, Massachusetts, 1983).

Originally conceived as an alternative to regular party politics and as an environmental party, the Green movement attracts voters with many different political convictions, and the Party is characterized by a lack of cohesiveness. There are, however, strong roots to the student movement of the 1960s and the peace movement of the 1970s. [20] Since achieving national parliamentary representation, the Greens have become extremely leftist. Much of their legislative work in the *Bundestag* focuses on casting suspicion on NATO, criticizing the United States, discrediting the work of the German intelligence agencies, etc., while at the same time being very understanding with the Soviet Union. This is accomplished by a barrage of questions to the Kohl Government, the introduction of bills, and various procedural moves. Altogether, these techniques have a certain disruptive effect, but they have achieved little else. [21]

The majority fractions in the *Bundestag* have had a difficult time in protecting sensitive information from access by Green representatives. The problem was especially urgent with regard to the committees that exercise parliamentary oversight of the intelligence agencies. There are two such committees. One is the so-called Article 10 Law Gremium. It consists of five representatives appointed by a majority vote in the *Bundestag*. This group is regularly briefed on the wiretaps and electronic surveillance carried out by the intelligence agencies. [22] The other group is the Parliamentary Control Commission. It is appointed according to ordinary parliamentary procedures. This Commission is kept informed on the "general activities of the services" and on "events of particular significance." [23] When the 10th *Bundestag* convened in March 1983, the Greens were kept out of these two oversight committees by a majority vote of the coalition parties.

Another problem arose early in 1984, when it was time for the Budget Committee of the *Bundestag* to deal with the budget for the intelligence services. To prevent Green participation, the majority coalition proposed the establishment of a special committee of five persons to be elected by majority rule to deal with the budget for the intelligence agencies. [24] This

---

A description from the Greens' point of view is F. Capra *and* C. Spretnak, *Green Politics* (New York, 1984).

[20] *Supra* note 19, at 26-36, Pfaltzgraff.

[21] As can be seen from the parliamentary records of that period, e.g., *Deutscher Bundestag* [hereafter: BT] Drucksache 10/1864, 10/1923, 10/1786, and 10/1880, Plenarprotokoll 10/75, and many others.

[22] Gesetz zu Artikel 10 des Grundgesetzes vom 13. August 1968;, BGBl, I, p. 949, as amended by Gesetz vom 13. September 1978, BGBl, I, p. 546.

[23] Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes vom 11. April 1978, BGBl, I, p. 453.

[24] BT Plenarprotokoll 10/3 and 10.6.

majority proposal was adopted by a vote of 270 over 210, with the Social Democrats on the side of the Greens. Both the Greens and the Social Democrats contended that these decisions were undue infringements on parliamentary minority rights.[25]

These incidents illustrate the difficulties arising from the parliamentary representation of a new political party whose irrational and irresponsible conduct continuously raises the question of its credibility and trustworthiness.[26] On the other hand, the record of the Green Party is not likely to increase this Party's chances for future successes.[27]

Many of the actions of the Green Party are in conflict with some fundamental consitutional principles. Into this category fall the Green views on a grass roots democracy that should take over the functions of the duly elected or appointed organs of government. Of questionable constitutionality is also the Green espousal of illegal means of resistance to Government actions, and their attempts to involve local powers in the conduct of foreign policy, which is reserved to the Federation. These undemocratic methods and goals of the Greens have raised the question whether the Green Party should be declared unconstitutional in a proceeding before the Constitutional Court. So far, however, this step has not been taken by the Government because it is felt that the Greens do not pose an imminent danger, and that the discussion with the Greens should be carried out through the democratic process. On the other hand, it has been suggested that civil servants who are members of the Green Party should be investigated as to their loyalty.[28]

IV. Procedures in Personnel Security Investigations

The procedures and methods of personnel security investigations are laid down in internal regulations that are kept secret. Occasionally, however, some fragmentary glimpses of these are revealed in parliamentary sources, newspaper articles, and scholarly writings. This has been the case with the Guidelines of February 15, 1971, which were still reported as effective at the beginning of 1984, [29] although their reform and imminent replacement has been announced for years.

---

[25] BT Drucksache 10/988 and BT Plenarprotokoll 10/56.

[26] F. Fromme, "Die Heimsuchung der Irrationalität," FAZ, December 21, 1984, p. 1.

[27] *Supra* note 19, at 105 Pfaltzgraff.

[28] R. Stober, "Grüne und Grundgesetz," 16 *Zeitschrift für Rechtspolitik* [ZRP] 209 (1983). For the contrary view, *see* F. Hase, "Die Grünen -- eine verfassungsfeindliche Partei," 17 *ZRP* 86 (1984).

The 1971 Security Investigations Guidelines have been developed through various stages and revisions since 1955, when the Federal Republic became a NATO partner. The Guidelines were designed to live up to NATO requirements, and the procedures were tightened in the 1960s in reaction to the espionage cases of the period. Interest in the Guidelines surged in 1974, when the "Chancellor's spy," Günter Guillaume, was uncovered (see above). The Guillaume case was investigated by a Parliamentary Committee which published its findings and in the course of these gave some insights into the Security Investigations Guidelines of 1971. [30] From this report and some other sources, [31] the following picture emerges with regard to federal employees. [32]

The Security Investigation Guidelines are closely connected with the rules for the protection of classified information, and the scope of individual investigations depends on the degree of access to be granted to the investigated person. The purpose of the investigation is to uncover any circumstances that would indicate that the investigated person is a security risk, either because of his political circumstances or his character traits.

Defined as political risks are any circumstances in the conduct of an employee that raise questions about his allegiance to a free democratic order. This formula is directed both against right-wing and left-wing radicals. Considered as particularly hazardous are close connections to East Germany or to other countries under Communist rule. If a person has spent considerable time behind the Iron Curtain or cannot give sufficient data to allow a thorough investigation, these circumstances will be considered as "other security risks, for which the investigated person is not at fault." Character risks are described by a few examples such as extravagance in handling money, a passion for gambling or betting, a tendency to gossip about confidential matters, and "abnormal conduct in sexual matters."

The investigation is carried out by the security office of the employer. As a rule, this office is also in charge of the employee's security files. Generally these are not kept with the personnel files. The investigation of an individual begins with a security declaration and a questionnaire that he has to fill out. The questionnaire is very lengthy, and it asks for a detailed curriculum vitae with dates of employment, changes in residence, memberships in organizations, and similar information needed to trace a person's history. Information is also requested concerning third persons, particularly close relatives, and character references must also be given.

---

[29] Sechster Tätigkeitsbericht des Bundesbeauftragten für Datenschutz [hereafter: TB] BT, Drucksache 10/877, at 41.

[30] BT Drucksache 7/3246.

[31] Supra note 29; BT Drucksache 7/3083; F. Fromme, "Vorkehrungen gegen einen neuen Guillaume," FAZ June 19, 1979, p. 10. A reputedly useful source that was not available for this report is R. Riegel, Datenschutz bei den Sicherheitsbehörden (Stuttgart, 1980).

[32] For defense personnel, employees of the Federal Intelligence Service, and employees of the Länder, there may be some deviations.

The evaluation of security risks is carried out by the employer who should be briefed by his security officer. To evaluate political risks, the Federal Constitution Protection Office (BfV) is involved, which reports to the employer "whether there are any misgivings about the person's employment in a security-sensitive position." Persons who have been successfully cleared must be reinvestigated every five years.

The investigations are carried out at two levels of intensity. For persons with access to information classed TOP SECRET or COSMIC TOP SECRET, an extensive agency check is carried out which may also extend to the person's spouse or betrothed. In addition, a background investigation is carried out by agents who interview persons who are in a position to give information, including but not limited to the character references. For persons with lesser clearances, only the extensive agency check is carried out.

The extensive agency check is conducted by the Federal Constitution Protection Office, which searches its data banks and files. Then, other security agencies are requested to conduct a search of their systems and sources. Among them are the two other intelligence services, perhaps intelligence agencies of the Allies, and in any event the Constitutional Protection Offices of the länder where the person has resided during the previous ten years. These agencies in turn will query the local police agencies, who will undoubtedly involve the federal police information systems. The participating agencies will search for all available information without cut-off dates.

Since the Guillaume case, there has been talk about the necessity of reforming the 1971 Guidelines. A commission of government experts [33] reviewed the Guidelines in the light of the findings in the Guillaume Case and concluded in November 1974 that one reason for the breakdown of the system was the excessive amount of classified material requiring too many clearances. [34] According to the Commission, the inflated need for clearance proceedings overworked the involved agencies and made it impossible for them to give enough attention to the cases deserving a more thorough investigation. To remedy the situation, it was recommended to have a three-tier system whereby persons with exposure to confidential information would only undergo a simplified agency check with the BfV. By 1979 more than a dozen drafts for new guidelines had been prepared, and at the beginning of 1984, the 1971 Guidelines were still in effect. Among the controversial problems have been the evaluation of refugees from the East Bloc, the inclusion of nonmarital partners into the scope of investigation, and issues of data protection and due process.

---

[33] BT 7/3083.

[34] One expert, Fromme, supra note 31, suggests that the true reason for the Guillaume scandal was political pressure: Guillaume had been a valuable party worker in the Social Democratic Party, and the Chancellor wanted an expeditious decision on his clearance. The commission reports (supra notes 2 and 3) bear out this analysis: two agencies had raised the possibility that Guillaume was an East German agent. However, their suggestions were buried in the files, and a positive result was reported to the Chancellor.

V. Due Process in Security Investigations

The 1971 Guidelines provide some due process protections for the investigated person. In particular, a person must be told of any detrimental findings against him, and he must also be given a hearing to defend himself against any allegations. This rule may not be circumvented by unannounced investigations. The Guidelines guard against any clandestine investigations that exclude a person from a sensitive position without letting him know that he was dropped on security grounds. This is accomplished by prohibiting any investigations before the person has answered the questionnaire. From that point on, he has notice of the investigation and also consented to it. There is, however, some evidence that these due process requirements are not always observed by the agencies. [35]

A person who is under suspicion must be given enough information to carry out his defense. [36] However, no access to the security file itself is given. This limitation is an important exception from the general principle of German civil service law that employees have access to their personnel records. [37] The issue has been tested in court, and the courts generally hold that the separation of an employee's security file from his personnel file is justified in the interests of national security, which justifies the secrecy of informers. In a 1978 decision, the Federal Administrative Court summarized these reasons as follows: [38]

> Security files must be kept secret by their very nature because their disclosure would seriously endanger public interests and obstruct the implementation of public responsibilities. As pointed out by the appellate court, the need for secrecy is primarily albeit not exclusively mandated by activities of the Constitutional Protection Office. Its working methods and procedures, like the protection of informers and the preservation of the cooperation with friendly intelligence services, require the utmost discretion.

---

[35] *Supra* note 29.

[36] U. Battis, *Bundesbeamtengesetz* 522 (München, 1982).

[37] Sec. 90, Bundesbeamtengesetz [BBG] in der Fassung vom 3. Januar 1977, BGBl., I, p. 1, as amended.

[38] Decision of Bundesverwaltungsgericht [BVerWG] of January 26, 1978, 93 *Deutsches Verwaltungsblatt* [DVBl] 606 (1978).

VI. The Role of the Intelligence Agencies

A. General

The Federal Republic has several intelligence services, and they all are involved in personnel security investigations. The three federal agencies are the Federal Office for the Protection of the Constitution (BfV, *Bundesamt für Verfassungsschutz*), in charge of internal security, the Federal Intelligence Service (BND, *Bundesnachrichtendienst*), in charge of external security, and the Military Defense Agency (MAD, *Militärischer Abschirmdienst*, in charge of military security. Also, each of the *länder* has a constitutional protection office. Of these agencies, MAD clears military personnel, the BND clears personnel of its own agency, and the constitutional protection offices assist the other government agencies. All these agencies assist each other and also obtain help from the police.

In recent years, however, the work of the intelligence agencies has become the target of much legal and political controversy, and the discussion has been fueled by a series of incidents in which the agencies have been exposed for allegedly improper conduct. Among the widely publicized scandals was an eavesdropping operation during 1975 and 1976 in the prison of Stammheim to overhear conversations between terrorists and their attorneys, and an eavesdropping operation against a scientist, Dr. Klause Traube, suspected of terrorist connections. [39] The Traube case was particularly damaging to the Federal Constitution Protection Office. Together with BND, the Office planted eavesdropping devices in Dr. Traube's home, under the assumption that it was monotoring a connection between terrorists and a nuclear physicist with access to nuclear facilities. The Office was wrong on both counts, since Dr. Traube was a mechanical engineer and had no contacts with terrorists. [40] A recent scandal that brought much damage to the Military Defense Service was the case of General Günter Kiesling. In the fall of 1983, he had been termed a security risk for alleged homosexual conduct on the flimsiest of evidence. This case brought considerable embarrassment to the Kohl Government and led to parliamentary investigations that resulted in a promise of the executive branch of government to rewrite the security risk criteria. [41]

Critics of the intelligence services generally contend that intelligence operations violate the civil liberties and due process protections that are embodied in the Constitution. In particular, they claim that the intelligence services are based on insufficient statutory authorizations, that the assistance between intelligence agencies and other security agencies is illegal, and that many intelligence operations violate data protection. Before examining these charges, a description of the agencies and their legal framework may be helpful.

---

[39] B. Schlink, *Die Amtshilfe* 268 (Berlin, 1982).

[40] H.V. Bergh, *Köln 4713*, 423 (Würzburg, 1981).

[41] In response to a parliamentary question, a spokesman for the Federal Ministry of Defense stated on March 2, 1984, that the guideline for security investigations was under review, and that the term *sexual deviation* would be replaced by the phrase, "sexual conduct that may lead to blackmail." BT Drucksache 10/1101.

B. The Offices for the Protection of the Constitution

Of the three federal intelligence services, only the Federal Office for the Protection of the Constitution (BfV) was created by a specific law [42] and it was even authorized by the Constitution. [43] The BfV was created in 1950, in close cooperation with the allied powers, who, in governing postwar Germany, were influential in shaping the present system of security agencies. In particular, the allied powers wanted to prevent the reemergence of a secret police in the fashion of Hitler's Gestapo (Geheime Staatspolizei) which wielded unchecked police powers in the pursuit of political goals. [44] Yet, the postwar years clearly indicated the need for a domestic intelligence agency to deal with the threat of communist subversion. [45]

This issue was debated at length in the drafting of the Bonn Constitution, and a solution was sought to the dilemma of excessive police powers versus internal security. The problem was resolved by creating an internal security agency whose purpose was the protection of the Constitution, rather than a particular regime, and whose methods of operation were limited to the observation and collection of information on subversive activities. This ageancy was separated, in accordance with the British model, from any executive police powers, such as arrests, searches, seizures, etc. [46] Also, decentralization was ensured by creating equivalent offices in each of the länder and by providing for cooperation between them and the Federal Office. All these principles were laid down in the Federal Constitution Protection Law of 1950. [47]

In 1972, this Law was amended to expand the powers of observation over some activities of aliens within the Federal Republic. At the same time, the function of the constitution protection offices was described in more detail to assure their legality at a time of increased emphasis on privacy laws. [48] Since then the Federal Law describes the general functions of the constitution protection offices as the "collection and evaluation of information, intelligence, and other data" on:

---

[42] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes [BVerfSchG] vom 27. September 1950, BGBl, I, p. 682, as amended by Gesetz vom 7. August 1972, BGBl, I, p. 1382.

[43] Art. 87, para. 2, GG.

[44] E. Litchefield, 2 Governing Postwar Germany 407 (Port Washington, 1972).

[45] W. Imle, Zwischen Vorbehald und Erfordernis 106 (München, 1984).

[46] Supra note 44, at 417.

[47] Supra note 42.

> 1. Efforts directed against a free and democratic basic order or against the existence or security of the federation or one of the lHnder or efforts aiming at illegally impairing the official functions of members of constitutional organs of the federation or the lHnder;
>
> 2. Security-endangering or intelligence activities carried out within the jurisdiction of this law on behalf of a foreign power;
>
> 3. Efforts within the jurisdiction of this Law, which endanger foreign affairs interests of the Federal Republic by the use of force or through actions preparatory therefore.

This description of the purposes and methods of intelligence work has in the meantime also become relevant for the other intelligence services that do not have an authorizing law (see below).

With regard to personnel security investigations, the Federal Law also has become more explicit in 1972, and the role of the consitutional protection offices in this field is described as the "participation" in:

> 1. The investigation of persons who, in the public interest, are entrusted with facts, objects, or knowledge that require secrecy, or who are to be granted access to these or can otherwise obtain it;
>
> 2. The investigation of persons who are or are about to be employed in security-sensitive positions in installations that are important to defense or in other ways essential. [49]

Similar passages are contained in the lHnder laws on consitutional protection.

The BFV is organized into seven divisions and one each of these deals with right-wing extremism, left-wing extremism, discovery of espionage, protection of secrecy, dangerous activities of aliens, and terrorism. One division maintains the data base of the Office (Nachrichtendienstliches Informationssystem, NADIS). This system stores and retrieves all obtained information relevant to internal security. [50]

---

[48] H. Evers, in Bonner Kommentar, art. 73, No. 10 (Hamburg, 1974).

[49] Sec. 3, BVerfschG.

[50] A. Schoreit, Innere Sicherheit in der Bundesrepublik Deutschland 60 (Heidelberg, 1979).

Each year the BFV prepares a report on the internal security situation which describes dangerous groups on both the right and the left. These annual reports are published by the Federal Minister of the Interior. [51] Although the reports are useful in terms of informing the public of recent developments, they often become political issues. For instance, the 1978 report, published by the Schmidt Government in 1979, was criticized for being too soft on communism. Whereas the 1972 report had clearly traced that the new Communist Party, DKP, was identical with the old prohibited KPD, no such mention was contained in the 1978 report, allegedly for the purpose of maintaining good relations with the East Bloc. [52]

C. The Military Defense Service

The Military Defense Service, MAD, was established in 1956, at the time of the creation of the German Armed Forces (Bundeswehr). MAD was not created by a specific law. Instead, its organization and working methods are regulated by internal, nonpromulgated regulations of the Federal Minister of Defense, to whom MAD is subordinated. The legal justification for this method of creation is found in the powers of the Federation to organize the Armed Forces and the powers of the Defense Minister to command them. [53]

The primary function of MAD is to protect the armed forces against espionage, subversion, and sabotage; and, within this scope of activities, MAD is responsible for the personnel security investigations within the armed forces. These investigations are carried out according to guidelines that have been written in coordination with the other NATO countries. [54]

The work of MAD is shrouded in much secrecy, and in the absence of enabling legislation, the scope of the agency's activities is the subject of much controversy. There is agreement that MAD, like the other intelligence services, has no police powers and is limited to intelligence operations. Like the constitution protection offices, MAD collects domestic information, and there is a certain overlap between these agencies. MAD is specifically mentioned in the Parliamentary Control Law of 1978, which subjects all intelligence services to the oversight of the Federal Diet, [55] and MAD is also mentioned in the law which permits exceptions to the constitutional secrecy of telecommunications and the mail. [56] Within the limits provided by this Law, MAD can use wiretaps. Outside of this statutory power, however, there is much debate on the propriety of other intelligence measures. [57]

---

[51] Supra notes 14 and 18.

[52] FAZ, July 12, 1979; FAZ, September 18, 1979.

[53] Arts. 65a and 87a, GG.

[54] G. Gusy, "Der Militärische Abschirmdienst," 36 Die öffentliche Verwaltung [DOV] 60 (1983); supra note 50, at 62.

[55] Supra note 23.

D. The Federal Intelligence Service (BND)

BND is in charge of foreign intelligence. Its domestic operations are limited; however, it can engage in domestic operations when monitoring foreign activities within the Federal Republic, and the agency also carries out its own personnel security investigations.

Officially established in 1955 by an internal (nonpublished) decree of the Federal Chancellor, BND was actually formed during the occupation regime through the U.S. sponsorship of Reinhard Gehlen's organization. [58] The legal situation of BND is similar to that of MAD. There is no enabling legislation outside of the specific mentions in the parliamentary control law and the wiretap law, and BND is subject to the same critical review as to the legality of its operations as MAD. [59]

VII. Restrictions on Interagency Cooperation

Until a few years ago, the intelligence services received much useful information from the various police agencies. Under the German principle of "administrative assistance," regular programs of cooperation had been established between the various agencies, which were carried out according to unpublished guidelines. Late in the 1970s, however, the unpopularity of the intelligence services focused much attention on the cooperation between the security agencies which has led to a change in the internal rules governing it. To date, the controversy continues with demands for a more restrictive practice on one side and an insistence on the need for information on the other. [60]

Among the criticized programs was a connection between the BfV information system, NADIS, and the data banks of the Federal Criminal Office (Bundeskriminalamt). The latter has some very sophisticated computerized systems, including the INPOL system which generally assists the police in their investigations, and the PIOS system which specializes in terrorist affairs. Also, it had become known that police and constitutional protection officials had regular meetings and that the latter disguised themselves as policemen in order to observe demonstrators.

---

[56] J. Carr, "Wiretapping in West Germany," 29 American Journal of Comparative Law [Am. J. Comp. L.] 617 (1981).

[57] *Supra* note 54, Gusy; R. Riegel, Polizei- und Ordnungsrecht 92 (Heidelberg, 1981).

[58] E. Cookridge, Gehlen, Spy of the Century 142 (London, 1972).

[59] *Supra* note 57.

[60] H. Kalkbrenner, "Amtshilfeproblematik im Verhältnis Polizei-Verfassungsschutz," in Polizeilicher Eingriff und Grundrechte 72 (Stuttgart, 1982).

Inter-agency cooperation even led to the resignation of a federal minister in 1978, when it became publicly known that the Border Protection Service (Bundesgrenzschutz, BGS) regularly assisted the BfV by monitoring the traffic between East Germany and West Germany. The BGS officials interrogated travellers as to the purpose of their travel, copied visas in passports, and searched luggage for subversive literature. [61] This practice was restricted by a rewriting of the guidelines in 1979, which since then only permit the notification of the BfV as to East German functionaries and business travelers and those persons suspected of espionage.

The proponents of inter-agency cooperation find it justified by Article 35 of the Constitution which provides that:

> All federal and land authorities shall render each other legal and administrative assistance.

Critics of the practice contend that the constitutional concept of administrative assistance is being abused to circumvent the separation between intelligence work and police work as expressed in the Law on Constitution Protection:

> The Federal Office for the Protection of the Constitution does not have police authority or control powers. To carry out its functions according to paragraphs 1 and 2, it is authorized to employ means appropriate for intelligence services. The Office may not be integrated into a police office. [62]

This separation between intelligence work and police work is a fundamental principle governing German security agencies. The separation is two-fold: the police agencies and intelligence agencies not only have different purposes but also use different means to achieve them. The police act when there is a specific suspicion that a crime has been or is about to be committed, whereas the intelligence agencies act in a more generally preventive way to guard against any future dangers. The police have been given specific powers of search, seizure, and interrogation which are subject to judicial controls and to some extent are carried out openly.

The intelligence agencies, on the other hand, have no coercive powers and are limited to the "means and methods appropriate to intelligence work." Although these methods are not enumerated in any law, they undoubtedly include observations, interrogations of third persons, the infiltration of associations by informers, and some forms of electronic surveillance. To be effective, these methods must be secret, and some scholars altogether have questioned the constitutionality of these measures. [63]

---

[61] *Supra* note 39.

[62] Sec. 3, para. 3, BVerfSchG.

However, even among those that affirm the legality and necessity of the intelligence-gathering methods, there is agreement that the intelligence services are not permitted to break the law, and that an unbridled and uncontrolled cooperation between police and intelligence agencies would lead to a system of surveillance that endangers civil liberties. [64] Nevertheless, there is much disagreement on where to draw the line, and no easy solutions have been found so far on how to achieve the proper balance between effective intelligence work and the protection of civil liberties. [65]

VIII. The Impact of Data Protection

The wave of privacy legislation that swept the western world in the 1970s also had its effect on the Federal Republic. There, the threat to personal liberty was seen as resulting from the capabilities of the computer to store personal information, to retrieve it, and to combine it with other computerized files. It was feared in Germany that the unbridled activities of private and governmental data banks would make the individual "transparent," by allowing the data processors to form a picture of his habits, living patterns, likes and dislikes, and other matters that fall into the protected sphere of privacy. [66] To guard against these dangers, a Federal Data Protection Law was enacted in 1976, [67] and by 1981 all the *länder* had also enacted similar laws.

In essence, the Federal Data Protection Law guards against the abuse of personal data in both private and governmental automated data processing systems. This is accomplished by limiting the electronic processing of personal data to cases where this has been permitted by law or by the consent of the data subject, by giving the individual a right to be informed about the data stored on him, by requiring the data processor to protect the confidentiality and accuracy of the data, and by employing data protection officials to monitor these matters within the enterprise.

Government agencies must inform the public of the data processing systems maintained by them, and this notification must describe the types of data, the circle of persons involved, the purposes for which this information is needed, and what transfers will be made to other agencies. Upon request and payment of the costs, government agencies must inform any person about the data stored on him. The individual has the right to demand the correction of wrong data and the erasure or blockage of data not rightfully needed by the agency. The Federal Government also had to appoint a Federal Data Protection Official, and this person has to monitor compliance with the law, report any deficiencies and make recommendations for improvements. To accomplish this, the official has far-reaching powers of inspection, and he publishes an annual report on his activities. In addition, the official also assists private individuals in any problems they may have with agencies that process their data.

---

[63] W. Schatzschneider, *Ermittlungstätigkeit der Amter für Verfassungsschutz und Grundrechte* (Frankfurt, 1979).

[64] *Supra* notes 60 and 61.

[65] *Compare*, for instance, the contributions of W. Gansser *and* R. Riegel *in* "Zusammenarbeit von Verfassungsschutz und Polizei," 114 *Bayerische Verwaltungsblätter* 711 (1983).

[66] H. Bieber, "Die Diktatur der Daten," *Die Zeit*, May 12, 1978.

[67] Bundesdatenschutzgesetz [BDSG] vom 27. Januar 1977, BGBl. I, p. 201.

The intelligence services, as well as the police agencies, are exempt from the requirements of giving notice of their computerized files, and they are under no duty to give information to individuals about the data stored on them.[68] These exemptions were justified by the drafters of the Law on the grounds that the work of the security agencies requires secrecy and that any information rights against these authorities could be used by criminals, foreign agents, and persons engaged in subversive activities to find out what is known about them.[69]

Although the intelligence agencies are exempt from the information and notification requirements of the Federal Data Protection Law, they have nevertheless been seriously affected by the Law. The Federal Data Protection Official includes the security agencies (police and intelligence services) in the scope of his investigations; and he continually urges a more restrictive practice in the collection, storage, and transfer of data. He also monitors the observance of due process requirements in personnel security investigations.[70] In the *länder*, the situation is similar. Each land has a data protector, and all these officials are very critical of the security agencies.

The security agencies, on the other hand, resent the interference with their work by the data processor. In particular, they feel that the demand for the erasure of records no longer deemed relevant is at times hasty and short-sighted. For instance, in the late 1970s, a central file on violent demonstrators was erased, on the grounds that terrorism had largely subsided. Shortly thereafter, many criminal incidents took place that were carried out by demonstrators.[71]

Altogether, data protection has remained a controversial topic. When the Federal Law was first enacted, there was little public concern about the dangers of data processing. Instead, the impetus for the Law came from a small group of experts. In the meantime, the circle of experts in government, industry, and academia has increased. There has been a proliferation of literature, conferences, etc., most of which advocates more protection. Due to this continuous publicity, the public has become more suspicious of the government's handling of information, and several laws have been hampered or forestalled, such as the proposed legislation on machine-readable identification cards or that on improvements in the registers of residency.

---

[68] Secs. 12, para. 2, *and* secs. 13, para. 2, BDSG.

[69] BT Drucksache 7/1027.

[70] Recounted in the annual reports of the Federal Official, e.g., *Erster Tätigkeitsbericht* (Bonn, 1979); 6. TB, BT Drucksache 10/877.

[71] F. Fromme, "Teures Spielzeug Datenschutz," FAZ February 10, 1981; FAZ November 7, 1984.

These issues culminated in 1982 when a Census Law was passed.[72] In the course of the 1983 census, personal information was to be solicited from the population, including data on personal status, domestic relations, religion, citizenship, housing, occupation, etc. The primary purpose of the information was statistical, yet the Law also permitted the use of the data for the correction of the local residence registers and the release of some data to local authorities who were to limit its use to planning purposes. The Census Law was met with public apprehension that envisioned the creation of a surveillance state of Orwellian proportions.[73] The Law was challenged in the Constitutional Court, which in December of 1983 came down with a landmark decision. The Census decision[74] struck down the portions of the Law that dealt with the transfer of data from statistical offices to other agencies. In doing so, the Court pronounced a new "right of informational self-determination," that is rooted in the Constitutional guarantees of personal liberty. In particular, the Court held that:

> under the modern conditions of data processing, the protection of the individual against the unlimited collection, storage, use, and transfer of his personal data is encompassed in the general right of personality of article 2, paragraph 1, of the Basic Law in conjunction with article 1, paragraph 1.
>
> Limitations of this right to "informational self-determination" are permissible only when there is a preponderant public interest. In accordance with the Constitution, they require a statutory foundation that must live up to the due process requirement of unequivocal legislation. In such rules, the legislator must also live up to the principle of proportionality. Also, he must provide for organizational and procedural measures that counteract any danger of a violation of the right of personality.

In the aftermath of the Census decision, the proponents of increased data protection have upgraded their efforts in favor of more restrictive legislation. Particularly, they feel that the decision contains a clear mandate to enact laws on the intelligence services so far regulated by executive decrees, as well as restrictive legislation on interagency cooperation, and more stringent data protection laws. 75/ However, the critics of the Decision find that the new right of "self-determination" lacks a foundation in the Constitution and has instead been created by demands in the data protection literature rather than by sound reasoning. 76/ Also, the Kohl Government feels no great urge to rush into major reforms in this sector on the grounds that the new constitutional right is not clearly enough defined to lead to statutory reforms. 77/

---

[72] Volkszählungsgesetz 1983, vom 25. März 1982, BGBl, I, p. 369.

[73] FAZ, October 12, 1983.

[74] BVerfG decision of December 15, 1983, 10 *Europäische Grundrechte Zeitschrift* [EuGRZ] 577 (1983).

IX. The Loyalty of Civil Servants

In the Federal Republic, civil servants must show allegiance to the basic tenets of a free and democratic order. This duty of loyalty extends to the career officials (*Beamte*) as well as to the contractual employees in the two-tier civil service, although it is more clearly pronounced for the career officials. Also, this duty of loyalty governs both the civil servants of the federation and of the *länder*, although enforcement varies. 78/ Altogether, this duty of loyalty has been interpreted to exclude persons from civil service who participate in associations or activities that clearly violate the fundamental principles of a democracy.

For the federal career officials, the duty of loyalty is expressed as a criterion for appointment:

> A person may only be appointed to the Civil Service if he offers surety that he at any time will intercede in favor of the liberal democratic order within the meaning of the Constitution. 79/

75/ "Auswirkungen des Volkszählungsurteils," *in* 37 DOV 505 (1984); R. Riegel, "Auswirkungen," *in* 31 *Recht im Amt* [RIA] 121 (1984); Gesetzentwurf der Fraktion der SPD, Entwurf eines Gesetzes zur anderung des Bundesdatenschutzgesetzes, BT Drucksache 10/1180.

76/ H. Schneider, "Anmerkung," 37 DOV 161 (1984); *see* also, *supra* note 39, at 171.

77/ F. Steinmeyer *and* B. Zypries, "Informationsgesellschaft oder Uberwachungsstaat," 12 *Demokratie und Recht* 307 (1984). There is, however, internal disagreement within the Kohl coalition government on the importance of new data protection legislation. As of December 1984, the Free Democratic Party was holding up the passage of a law on a personal identification card by insisting on legislation to delimit the powers of the intelligence services: FAZ December 27, 1984.

78/ In the *länder*, the loyalty requirements are enacted by *länder* laws that remain within the framework of a federal law: Bundesrechtsrahmengesetz [BRRG] in der Fassung vom 3. January 1977, BGBl., I, p. 21.

79/ Sec. 7, para. 1, no. 2, BBG, BGBl, I, p. 1.

In addition, the duty of loyalty is expressed as an ongoing obligation [80] and a violation of this duty gives rise to a disciplinary proceeding that may lead to the civil servant's dismissal. Even retired civil servants remain bound by the duty of loyalty. [81] Civil servants must also swear an oath or otherwise make a solemn promise that they will uphold the Constitution and carry out their duties. [82]

The German insistence on the loyalty of the civil servants dates back to Prussian times, and critics of the practice are quick to point out the infamous role played by blind obedience in the Third Reich, when civil servants had to swear allegiance to the *Führer*. However, it should be noted that the current loyalty provisions are rooted in the suggestions of the American and British occupation governments following World War II.

In the late 1940s, the Western allies, particularly the Americans and the British, took an active interest in reshaping the German public institutions in a manner that would ensure a lasting democratic order and forestall the rise of another totalitarian movement. In this context, the organization of the German Civil Service became a major issue. The Allied Powers felt that the traditions of the German Civil Service were authoritarian and elitist, and many suggestions were made on how to remedy this situation. The Germans, on the other hand, wanted to retain many of their traditions. A compromise was reached in Article 33 of the Bonn Constitution, which upholds the traditional principles of the German Civil Service while tempering them with guarantees of nondiscrimination and equal opportunity. One of these traditional principles is the duty of loyalty. Yet, this tradition was wholeheartedly supported by the Western allies. In fact, a Military Control Law issued by the Bizonal (American-British) Government in 1949 regulated the German Civil Service and it contained an allegiance clause almost identical to the one later enacted in the 1953 Civil Service Law of the Federal Republic. [83]

Throughout the 1950s and 1960s, civil servants were expected to live up to loyalty requirements, and contrary behavior was both a reason for nonselection or dismissal. The practice was based on a decree of the Federal Government that listed several radical organizations of the right and of the left, including the Communist Party (KPD, *see* above).

---

[80] Sec. 52, para. 2, BBG.

[81] Sec. 77, BBG.

[82] Sec. 58, BBG.

[83] *Supra* note 44, vol. 1, at 272.

In 1972, the practice of the German governments in the Federation and the länder was formalized in the so-called Radicals Decree. [84] It provided that:

> 1. an applicant who is engaged in anticonstitutional activities shall not be admitted into the civil service, and
>
> 2. a person's membership in an organization that pursues anticonstitutional goals shall create doubts as to his readiness to stand up for a free democratic order and as a rule may lead to a denial of the application.

In practice, this decree was implemented by making routine inquiries with the offices for the protection of the constitution. If there were detrimental findings on a person, he was granted a hearing to clear himself. If he was denied employment, the reasons therefore were stated together with an instruction on his judicial remedies.

By 1972, the Radicals Decree had become necessary to justify the governmental practice, because the courts had developed the constitutional guarantees of equal access to the civil service into a right to be given a reasoned decision for a denial of employment. The issuance of the Radicals Decree, however, did not resolve the problem. Instead, it unleashed one of the most bitter and protracted legal and political controversies in the constitutional history of the Federal Republic. [85]

In 1975, the issue was tested in the Federal Constitutional Court, and in the so-called Radicals decision, [86] and the Court affirmed the government's right to insist on the loyalty of its civil servants.

The case involved a candidate for the preparatory civil service required for attorneys. The petitioner was denied employment by virtue of the loyalty requirement of a particular land, because he had participated in some 40 meetings of a student association with clearly antidemocratic purposes named Rote Zelle Jura (Law Student's Red Cell) and had also falsified election results for a student parliament. The petitioner claimed that this denial of his appointment violated his constitutional rights of due process and his basic right to chose a profession.

The Court held that insistence on the political loyalty of civil servants is justified by the common welfare and is mandated by the Constitution, and that it is part of the system of a "militant democracy" by which the Constitution allows a defense against antidemocratic forces. Also, the loyalty examination is an appropriate consideration of the suitability of the candidate, particularly since dismissal of a civil servant is a very cumbersome legal process. Moreover, the loyalty requirement applies to every civil servant, regardless of status or the importance of his position. With regard to political parties the Court held that even membership in a political party that had not been declared anticonstitutional (*see* above) could be a violation of the duty of loyalty if this party actually pursued antidemocratic goals. On the other hand, the Court raised the possibility that a land requiring a preparatory government employment as a prerequisite for bar membership of attorneys might provide candidates an opportunity to meet this requirement without civil service status.

---

[84] Bulletin der Bundesregierung vom 3. Februar 1977, p. 142.

[85] For a selected bibliography on the literature until 1977, see K. Stern, 1 Das Staatsrecht der Bundesrepublik Deutschland 282, note 130 (München, 1977).

[86] BVerfG decision of 22. May, 1975, 39 BverfGE 334 (1975).

The 1975 Radicals decision has since been followed by other court decisions, among them several that upheld the dismissal of civil servants who were members of the legal yet antidemocratic German Communist Party (DKP). In any event, dismissal is justified if the civil servant engages in continuous activities for an antidemocratic party, particularly if this conduct has occurred since the Radicals decision of 1975.[87]

Although the courts clarified the law on the loyalty requirement, the actual practice has changed in recent years. Due in part to the continuously bad publicity that the German Government was getting from the loyalty issue,[88] the Federal Government changed its procedures in 1979. The new guidelines are used in the Federal Government and in some of the *länder*.[89] They provide that routine inquiries on the conduct of all applicants are no longer permissible. Inquiries with the Constitutional Protection Office may be carried out only if an employee raises serious doubts during his initial temporary employment. In responding to any inquiries, the constitutional protection offices must restrict their replies to the furnishing of information that could be used as evidence in court; also, no information shall be given about a person's conduct before the age of 18. Moreover, information that is older than two years can be revealed only if this is justifiable under the constitutional principle of proportionality.

In March 1982, a further erosion of the loyalty requirement was proposed by the Schmidt Government. It introduced a bill into Parliament that would have limited the loyalty requirement to civil service positions of some importance.[90] It was proposed that "the functions entrusted to an official should be considered as well as his civil rights in adjudging whether a violation of the duty of loyalty committed by him in his private conduct should be adjudged a disciplinary matter." The bill reflected a lengthy debate on whether the loyalty requirement should be less intense for persons such as teachers and postal workers. However, the bill lost its chance for enactment when the Kohl coalition government was formed in the fall of 1982.

---

[87] The so-called Peters Decision, i.e., decision of the Bundesverwaltungsgericht of 29. October 1981, 30 *Zeitschrift für Beamtenrecht* [ZBR] 22 (1982).

[88] Criticism has not abated with the Radicals Decision. For a typical critique of that Decision, *see* W. Damkowski, "Radikale im Öffentlichen Dienst," 23 RiA 1 (1976).

[89] Grundsätze für die Prüfung der Verfassungstreue vom 19. Mai 1979, 6 EuGRZ 236 (1979).

[90] BT Drucksache 9/2058.

As could be expected, the European Human Rights Commission has also become involved in the German loyalty requirement for civil servants, although it has not as yet ruled on the merits of a case. However, in a 1982 decision [91] that quoted the U.S. Supreme Court's Keyishian decision, [92] the Commission indicated that it had jurisdiction in loyalty cases because they touched on the Convention's right of freedom of expression. [93] As of July 1984, two complaints were pending. [94]

X. Comparison with Other West-European Countries

By 1974, German scholars were claiming that the loyalty discussion was stagnating and that all worthwhile points had been made on both sides of the issue. [95] This remark still holds true, after another decade of discussion. However, an interesting side effect of this German debate is the German comparative literature on the topic. Studies have been published that compare the loyalty and security laws and practices in other West-European countries with the situation in West Germany. [96] Their conclusions differ — those that abhor the German practice find that no other countries have laws as repressive as the Federal Republic, whereas the defenders of the German loyalty requirement find that the other West-European countries have ways and means to screen out persons of radical political convictions from public employment.

Altogether, these studies indicate that most West European countries have issued few laws or published regulations on loyalty or personnel security in the Government. This is true, at least for Austria, Belgium, France, Italy, and Switzerland. Two notable exceptions from this lack of publicity are the Netherlands and Sweden. These two countries have published some very interesting guidelines on personnel security investigations. However, the amount of legislation on security and loyalty requirements are not necessarily an adequate gauge for the actual government practice.

---

[91] Decision of the European Human Rights Commission of December 16, 1982, 10 EuGRZ 411 (1983).

[92] Keyishian v. Board of Regents, 385 U.S. 589 (1967).

[93] This particular case was rejected by the Commission because the petitioner had not exhausted the domestic remedies. The petitioner was a German mathematician who had been denied a teaching position for his extensive involvement in communist politics.

[94] A. Bleckmann, "'Berufsverbote' und die Europäische Menschenrechtskonvention," 37 DOV 566 (1984).

[95] H. Weiss, "Die Verfassungstreuepflicht des Beamten," 22 ZBR 81 (1974).

[96] K. Doehring, *et al.*, *Verfassungstreue im öffentlichen Dienst europäischer Staaten* (Berling, 1960); E. Böckenförde, *et al.*, *Extremisten im öffentlichen Dienst* (Baden-Baden, 1981).

A cursory glance at the laws of Italy and France might indicate that these countries find the criminal laws sufficient to ensure personnel security. Both countries have strong Communist parties whose members are not barred from civil service employment, and political activity is generally allowed to civil servants. Also, these countries fill civil service positions on the basis of competitive examinations.

However, a closer look at these countries reveals some mechanisms that may operate to keep political extremists and other security risks out of government. In Italy and in France, civil servants are expected to comport themselves with a certain amount of political restraint. In France, extremist activity prior to a candidacy for public employment may prevent an applicant from being allowed to compete in the examinations. In Italy, the Criminal Code contains a long list of state-endangering offenses, and a criminal record prevents civil service employment.

In some smaller European countries, security risks may be kept out of government employment by the mere fact that they are locally known. This may be the case in Austria, Belgium, and Switzerland. In Austria and Belgium, moreover, the established political parties make sure that only their proteges will get government jobs. Deplorable though this practice may be, party sponsorship might eliminate security risks.

In all these countries, however, the government has retained a larger amount of discretion in the hiring of personnel than is the case in the Federal Republic of Germany. In these countries, judicial review for a denial of employment is either unavailable or very limited.

XI. Conclusion

Matters of personnel security must be resolved by each country within the framework of its legal system, historic conditions, and political realities. Bearing this in mind, the West German situation gives rise to a few considerations.

With regard to the loyalty issue, it seems that the official German position is quite reasonable despite the shrillness of its detractors. In view of the National Socialist past, and the proximity and special quality of the Communist threat, it does not seem excessive that civil servants are expected to profess allegiance to fundamental democratic values and to the Constitution. This Constitution has impeccable democratic credentials, and it has proven itself over the past 35 years by allowing for an unprecedented amount of personal freedom and a truly democratic plurality of political expression.

With regard to personnel security measures, the picture emerges of a government beleaguered by some very ambitious privacy demands that may hamper effective investigative techniques and prevent the adequate storage of information. These demands have been created and nurtured by a somewhat one-sided legal literature and they have found a resonance in the courts.

This German situation is somewhat reminiscent of the developments in the United States, particularly the line of cases from Greene v. McElroy [97] to Jane Doe v. United States Civil Service Commission. [98]

Countries with very high standards of due process and extensive possibilities for judicial review tend to have a difficult time in drawing the line between the protection of the individual and national security interests. Yet such a line must be drawn at some point. Reasonable people everywhere would agree that employment should not be denied or terminated on the basis of unfounded suspicions or unchecked accusations, yet the protection against these dangers should not destroy essential methods of investigative work. Security investigations cannot be effective unless confidential sources of information are protected from disclosure and unless data bases are maintained and used. These points need to be made in the public debate of these issues, lest we endanger the very foundations of our form of government.

---

[97] 360 U.S. 474 (1959).

[98] 483 F.Supp. 539 (1980).

BELGIUM

Prepared by Dr. George E. Glos
Assistant Chief
European Law Division
Law Library, Library of Congress
September 1984

In order to be appointed, all public servants in Belgium have to show that they are irreproachable in their conduct and are in possession of their civil and political rights. They also have to produce an extract of the criminal records showing no convictions.[1] Public officers and government contractors have to display a high degree of moral integrity and are exposed to criminal prosecution should they fail to act accordingly.

Provisions Concerning the Corruption of Public Officers

A public officer who receives a gift in order to exercise his official functions in an unjust manner or who abstains from making an official act will be punished by imprisonment from 3 months to 3 years and by a fine from 100 francs to 3,000 francs.[2]

If the public officer agrees to commit a felony or a misdemeanor in the exercise of his official functions, he will be punished by imprisonment from 1 to 5 years and by a fine from 200 francs to 5,000 francs.[3]

Anyone who has bribed a public officer will be punished by the same punishment as the one he has bribed. An attempt to bribe is punishable.[4] The money used to bribe will be confiscated and given to welfare.[5]

Public officers may also lose their office if they are found guilty of bribery.[6]

---

[1] Royal Decree of October 2, 1937, the Public Service Regulation, as amended, art. 16. J. Servais and E. Mechelynck, comps., 3 Les Codes Belges 29 (Bruxelles, Bruylant, 1983).

[2] Criminal Code, art. 247, J. Servais and Mechelynck, comps., 2 Les Codes Belges 55 (Bruxelles, Bruylant, 1983).

[3] Id. art. 248.

[4] Id. art. 252.

[5] Id. art. 253.

[6] Id. arts. 246-249.

The Abuse of Authority by Public Officers

A public officer who would use the authority of his office to prevent the operation of a law or a royal decree, the collection of taxes, the operation of a judicial order, or any other official order will be punished by imprisonment from 1 to 5 years. If his action was effective, he will be imprisoned from 5 to 10 years. If such an action was the direct cause of other felonies punishable more severely, punishment may be increased up to imprisonment for life.[7]

A public officer who ordered or undertook an act in breach of a law or a royal decree will not be punishable if he can show that he acted under superior orders. Those who gave the order are punishable.[8]

Provisions Concerning Suppliers

Any person entrusted with supplying, undertaking, or servicing on behalf of the armed forces who voluntarily fails to perform the service entrusted to him will be punished by imprisonment from 5 to 10 years and by a fine from 200 to 3,000 francs. The same punishment is applicable to the supplier's agents who have voluntarily failed to perform the service.[9]

Public officers or government agents who have induced the perpetrators to act or who have aided them in failing to perform the service will be punished by imprisonment of at least 7 years and by a fine from 300 to 3,000 francs.[10] If the service is interrupted because of the negligence of the suppliers, their agents, public officers, or government agents, those guilty will be punished by imprisonment from 3 months to 2 years and by a fine from 100 to 1,000 francs.[11] If, despite performance of the service, the delivery and the work has been voluntarily delayed, those guilty will be punished by imprisonment from 6 months to 2 years and by a fine from 200 to 1,000 francs.[12] If the delay is caused by negligence, those guilty will be punished by imprisonment from 1 month to 1 year and by a fine from 50 to 500 francs.[13]

If there is fraud in the nature, quality, or quantity of the work, labor force or the supplies, those involved will be punished by imprisonment from 6 months to 3 years and a fine from 100 to 10,000 francs.[14] Public officers or government agents who took part in the fraud will be punished by imprisonment from 2 to 5 years and by a fine from 200 to 10,000 francs.[15]

---

[7] Id. arts. 254-255.
[8] *Id.* art. 260.
[9] *Id.* art. 292.
[10] *Id.* art. 293.
[11] *Id.* art. 294.
[12] *Id.* art. 295.
[13] *Id.*
[14] *Id.* art. 297.
[15] *Id.* art. 298.

PERSONNEL SECURITY IN THE PUBLIC SERVICE OF CANADA

Prepared by Stephen F. Clarke
Senior Legal Specialist
American-British Law Division
Law Library, Library of Congress
April 1985

Prior to and during World War II, the federal government did not have any form of a standard security clearance program for public service employees. The need for personnel security was dramatically brought into focus in 1946 by a Soviet agent who, after he had been apprehended, revealed that the Soviet Union had been obtaining confidential information from high offices in the Canadian government for a number of years.[1] Included among the Canadians who had been secretly working for the Soviets was a member of the majority party in Parliament. The Canadian government responded, as it would several times again in the future, to public conern over the state of personnel security by appointing a commission to investigate the affair and to make recommendations as to how breaches of security could be prevented. One of the measures that this panel, the Taschereau-Kellock Commission, suggested was the implementation of standard security screening. In 1948, the federal cabinet adopted this recommendation by ordering the Royal Canadian Mounted Police (the R.C.M.P.) to conduct background checks on all candidates for employment in certain sensitive positions. The document containing this order, Cabinet Directive (C.D.) 4, was modified later in 1948 to prohibit members or associates of communist and fascist organizations from being employed in government positions requiring trust and confidentiality.[2]

C.D. 4 was replaced by C.D. 24 in 1952. This new order established two separate grounds for denying security clearances. The first of these grounds was disloyalty. Under C.D. 24 this ground was expanded to cover supporters of any ideology that advocated the overthrow of the government by force and certain other persons considered subversive. The second ground for denying security clearances in C.D. 4 was unreliability. A person was deemed by the order to be unreliable if he or she had a character flaw that made him or her susceptible to intimidation or blackmail.[3]

C.D. 29 superceded C.D. 24 in 1955. The new directive preserved the two grounds for denying security clearances and also extended the number of positions that required a security clearance to include virtually all employees having access to classified information. In the late 1950's and the early 1960's, the security screening program came under criticism from individual employees and in the media for being unflexible and unfair to certain groups. The federal cabinet responded to these criticisms by replacing C.D. 29 with C.D. 35, the last cabinet directive that would be adopted under what would become the old system in 1984. This latter document, the contents of which were kept secret until 1978, required the government to inform most persons denied security clearances that their reliability or loyalty was in doubt, and it also provided for some reviews of adverse decisions by a specially-created Board of Review. C.D. 35 also established more specific criteria for assessing loyalty and reliability than had been the case under the previous directives.[4]

---

[1] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Freedom and security under the law, 781 (1981).
[2] Id. at 782.
[3] Id.

Although C.D. 35 had introduced some reforms intended to protect the reputations and careers of individuals, public criticism of the personnel security system continued and led to the creation by the federal government of a Royal Commission on Security in 1966. This Royal Commission made a number of recommendations for changing the system and practices followed in personnel checks. One major suggestion was that a Security Review Board should be established to review denials of clearances, and another was that an individual's support for separatism in Quebec should not be reported or recorded unless that individual evidenced support for illegal or subversive activities. Neither of these recommendations was followed by the federal government, although provisions for appealing dismissals were made in 1978.[5]

Under C.D. 35, the Security Service branch of the R.C.M.P. continued to be responsible for investigating employees and applicants for employment, reporting the results of the investigations to department heads, and making recommendations to those department heads. These recommendations of the R.C.M.P. were not binding on department heads, each of whom could set his or her own standards, but they were followed in the vast majority of cases. The number of investigations that the R.C.M.P. was requested to conduct annually grew tremendously while C.D. 35 was in effect. In the years 1972-77, the average number of screening reports prepared was 67,000.[6] Clearances were given for access to three categories of protected documents. These three categories were top secret, secret, and confidential.

In 1977, as the result of growing reports and scandals involving numerous wrongdoings by the R.C.M.P. in the course of investigations over a number of years, the federal government appointed a Royal Commission to investigate the allegations and to make recommendations concerning their future activities and roles. In August of 1981, the McDonald Commission issued its final report on Freedom and Security Under the Law.[7] This extensive work reviewed the history of and the need for personnel security and contained numerous recommendations pertaining to personnel security. Many of these suggestions were very specific. In general, however, the Commission decided that the field of personnel security should be entrusted to a new government agency that should be given much clearer responsibilities and guidelines than the Security Service in the R.C.M.P. had been given. As to the extent of security of clearances, the Commission found that the great number required under Cabinet Directive 35 was unjustified, and that their frequency should be reduced to the minimum required to protect information that is critical to the security and defense of the country.[8] In this respect, the Commission found that many documents were being classified that could not be reasonably considered to contain information that should be kept in confidence. The Commission stressed the point that this was particularly true of materials marked "top secret."[9] In the same vein, the Commission recommended that the number of field investigations be reduced so as to allow investigators to do more thorough background searches in those cases where it was warranted or very important.[10] Finally, the McDonald Commission recommended, as had been done earlier, that a Security Appeals Tribunal should be created to reconsider denials of security clearances.[11]

---

[4] Id. at 783.

[5] VII Can. Consol. Regs. ch. 724 (1978).

[6] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Freedom and security under the law, 786 (1981).

[7] Id.

In May of 1983, the Liberal government headed by former Prime Minister Trudeau introduced legislation to create a new civilian security department to be called the Canadian Security Intelligence Service that would be responsible for the field of personnel security in the federal government. The proposed legislation was quickly and loudly attacked by civil libertarians for proposing to give the agency far greater powers than was warranted.[12] A committee of the Canadian Senate was appointed to review the legislation, and over forty changes were made to the original bill when it was reintroduced in the House of Commons in January of 1984.[13] The bill continued to be extremely contentious and was most vocally opposed in Parliament by the New Democratic Party. The New Democrats and, to a somewhat lesser extent, the Progressive Conservatives argued that the legislation would merely legalize many of the things the McDonald Commission had found that the R.C.M.P. had done earlier in violations of the law. Nevertheless, in the last days of Prime Minster Trudeau's long tenure, the Liberals invoked closure in the House of Commons and passed the Canadian Security Intelligence Service Act in June of 1984. On June 28, 1984, the Act received Royal asset, and it came into force in two parts in July and August of that year.[14]

The Canadian Security Intelligence Service Act contains ninety-six sections and fairly detailed provisions respecting the jurisdiction of the Service, the duties and functions of the Service, judicial controls of the Service, and appeals of decisions of the Service. Thus far, the Progressive Conservative Government of Prime Minister Mulroney has not yet adopted regulations to implement the Act. It has been reported that confidential new rules to replace C.D. 35 have been prepared for consideration by the federal cabinet, but no decision on these proposals have as yet been reached.[15] Thus, personnel security is a field that is still in transition as a new agency, the Canadian Security Intelligence Service, has taken over the responsibilities that were previously assigned to the Security Service of the R.C.M.P. and a new government, the Progressive Conservative Government headed by Prime Minister Mulroney, is preparing to consider new rules for security investigations under the Canadian Security Intelligence Service Act.

---

[8] *Id.* at 788.

[9] *Id.*

[10] *Id.*

[11] *Id.* at 808-812.

[12] XVI *Ottawa Letter* 160 (1983).

[13] XVI *Ottawa Letter* 461 (1984).

[14] Ch. *21, 1984 Can.* Stat. 615.

[15] Toronto Globe and Mail, Feb. 22, 1985, at 5.

FRANCE

Prepared by M. Tahar Ahmedouamar
Senior Legal Specialist
European Law Division
Law Library, Library of Congress
September 1984

The personal integrity of a government employee in France is determined by an inquiry before the individual is hired. Those people who have been convicted of felonies or even misdemeanors that relate to honesty are excluded from holding any public office. In addition, those employees or contractors who have committed some offenses or crimes in or out of the performance of their duties are removed from governmental offices or businesses.

According to article 23 of the law of October 1946, no one can be nominated to a public position if he does not show adequate integrity.[1] Before being permitted to compete for a position, an inquiry is made on a candidate by the administration. If facts that show a lack of integrity are revealed after competition, the candidate can still be excluded from the civil service in spite of the general rule which provides that after a person has been successful in a state competition he cannot be disqualified.[2]

The evaluation of the integrity of those interested in public employment may be made either through their behavior as civilians or even during the military draft, the way they exhibit their professional conscience, and their behavior towards the service and the taxpayers. Condemnations that have not benefited from an amnesty or condemnations that have tarnished the individual's honor and honesty are seriously taken into account.[3]

One rule that reinforces the integrity of government employees is the fact that the French civil service is based on the merit system which discourages favoritism, nepotism, returning favors, and kickbacks.

As a general rule, Article 6 of the Declaration of Rights of 1789, incorporated in the Preamble of the Constitution of 1958, provides that all French citizens are equally admissible to all public offices without any other distinction than those regarding their capabilities and talents.[4] The selection is based on competition which is open to persons who hold specific diplomas. Two major institutions, ENA and CPAC, prepare high civil servants for these examinations. These individuals are drawn mainly from those who have finished law school or a political science institute. They qualify for positions in category A.[5] Other candidates may enter categories B, C, and D. Diplomas and competition are required for all these categories, but competition is not mandatory for the lowest positions in category D.

---

[1] II Repertoire de droit public et administratif 128 (Paris, Dalloz, 1959).
[2] Id.
[3] Id.
[4] M. Duverger, Constitution et documents politiques 10 (Paris, P.U.F., 1974).

Promotion decisions are based on performance appraisals unlike step increases which depend on the time spent in the service.[6] The performance appraisal is based either on a competition in an examination open to all civil servants or is limited to a specific class of civil servants doing the same work or is based on a list of civil servants marked for promotion. This list includes the education, performance, evaluation made by the supervisor, and a scale of salaries. The list is revised each year and must be published in an official publication.[7] It is then submitted to the joint administrative commission. In case of a disagreement, it is possible to appeal the decision to the highest council of civil service. Also, an appeal is always possible to the supreme administrative court in a case involving the abuse or misuse of power against a civil servant in the field of promotion.

Personal integrity is also taken into account by excluding undesirable people from public office. The French Criminal Code prescribes different ways of losing one's civil rights, and this action automatically bars a person who works for the government in the Executive Branch directly or indirectly. This loss of civil rights includes, according to article 34 of the Criminal Code, the removal and exclusion of the convicted individual from all public functions, the prohibition to bear arms, to be a member of the National Guard, to serve in the French armed forces, and to be a school principal, teacher, or professor.[8] The latter field is important since French education is not private but state run. Article 42 provides that upon conviction of a misdemeanor, a court may, in certain cases, decree the loss of civil rights such as the right to be elected to a public office or to be able to exercise any function or employment in the government.[9] Pursuant to article 123, in addition to a jail penalty, a person who is already in the civil service may lose the right to exercise any public function for a period of time up to 10 years, if the person has acted unlawfully with other members of the government.[10] According to articles 166 and 167, every felony committed by a civil servant in the exercise of his official duties is a breach of duty and as such is subject to a loss of civil rights.[11] According to article 174, public officials who are guilty of extortion may be deprived of their civil rights and, thus, of the right to public employment for a period not exceeding 10 years.[12] Article 175 provides that civil servants may be punished by a perpetual loss of the right to hold public office in case they have participated in or received any part of a transaction involving public bidding in an agency under their partial or total control.[13]

---

[5] A. de Laubadere, Traite de droit administratif 64 (Paris, LGDJ, 1975).

[6] Id. at 66.

[7] M. Piquemal, 1 Le fonctionnaire (2nd ed., Paris, Berger-Lavrault, 1979).

[8] Code Penal 18 (Paris, Dalloz, 1981-82).

[9] Id. at 22.

[10] Id. at 86.

[11] Id. at 107.

People who deal with the government in matters concerning national security activities are of course held to higher standards. Thus, article 430 provides that any person entrusted either individually or as a member of an entity to supply or undertake on behalf of the army and fails to perform his service shall be punished by solitary confinement and a fine of no more than a fourth of adjudicated damages but not less than 1800 F.[14] According to article 431, suppliers and their agents may incur the same punishments as the one provided in article 340.[15] Article 432 states that if civil servants or employees of the government have helped the perpetrators in such a failure of service, they shall be punished by hard labor from 10 to 20 years.[16] Even when the service has been performed but through negligence the delivery and work has been delayed or if there was fraud concerning the quality or quantity of the work, workmanship or deliveries, the person who failed to perform adequately would be punished by imprisonment from 6 months to five years and by a fine of no more than one fourth of adjudicated damages but not less than 360 F.[17]

The personal integrity of those hired to work on national security activities such as military contracts for manufacturing weapons are very tightly monitored by governmental authorities. No chance is given by the law and general procedures to individuals or private firms to influence a contract in a direction that may be detrimental to the government or public interests. Thus, personal integrity is not blindly trusted but closely watched.[18]

The power of the government in relation to private companies can be clearly seen in all the series of authorizations allowing firms to start or stop manufacturing weapons at any given stage of production. First, the Decree of May 15, 1953 (added to the Second Decree of August 14, 1939), provides that a simple notification by the government of an order for war material placed with an enterprise that does not hold a manufacturing license or of an authorization for the sale of war material is the equivalent of a regular manufacturing license or sales authorization.[19] Therefore, an enterprise that receives such a government notification has no other choice but to abide by all the regulations during the time needed to fulfill the order. It is, of course, the government's prerogative to lengthen this period of time in order to keep the enterprise under the regulations that apply to the holders of licenses to manufacture or sell war material.

---

[12] Id. at 108-109.
[13] Id. at 110.
[14] Id. at 305-306.
[15] Id. at 306.
[16] Id. at 306.
[17] Id. art. 433.
[18] A. de Laubadere, I *Traite elementaire de droit administratif* 117-172 (Paris, LGDJ, 1971).
[19] Note 1, volume I at 147-148.

Second, the production or sales authorization may be revoked in any case of violation of war or work legislation and of all misdemeanors enumerated in article 12 of the Second Decree of August 14, 1939, and article 23 of the Decree of April 18, 1939.

Authorizations are granted in a discretionary way by the Minister of the Armies, and his freedom in this area is complete. A silence of 3 months following an application means a refusal to grant a license.[20]

Besides the procedures allowing government agents to monitor the manufacture of weapons, there is also legislation concerning the exportation of arms, once they are produced. The exportation of arms is governed by the Decision of June 13, 1956, following the Decree of July 16, 1955. The sanctions for exportation without authorization, or even for the attempt, fall under the penalties provided for by the Customs Code and under the sanctions provided by the Decree-Law of April 11, 1939.

The government's right to monitor private establishments is provided by the Decree-Law of April 18, 1939, article 2, and Decree B of August 14, 1939. In essence, those establishments that deal with the manufacture of and trade in any arms and ammunition (with the exception of those weapons that are of an historic nature or are collector's items) must, at the time of a factory's opening, sale, transfer, or closing make a preliminary declaration to the prefecture of the place where the business is located.[21]

The Decree-Law of April 18, 1939, divides war material in eight categories. For war material, arms, defensive weapons, and ammunition in categories 1 to 4, the manufacture of and trade in these items are subject to a preliminary authorization and to supervision by the state.

On-site inspections and book audits ("le controle sur place et sur piece") must be done by persons representing the departments (ministeres) involved (interesses). These agents, who are required to maintain professional secrecy, must supervise the manufacturing from both a technical and financial point of view including production, improvements in manufacturing, profits, and expenses for advertising and marketing (arts. 4, 5, and 9 of the Second Decree of August 14, 1939).

---

[20] Actualite juridique, Droit administratif, 1969, at 530.
[21] Id.

Articles 5 and 9 of the Second Decree of August 14, 1939, provide that for national defense reasons manufacturing licenses can be granted only to French citizens. This rule was modified by the Decree of August 24, 1956, which provides an exception allowing French companies with foreign associates to benefit from a manufacturing license or one of the authorizations mentioned in article 8.

The holder of the authorization must allow government agents without any interference to enter the enterprise and inspect the site, the material, and the financial records. The manufacturers must allow these agents to enter and investigate all parts of the enterprise. Furthermore, the holder of an authorization must provide all the data requested and communicate them to the government agents within 8 days after the registration of the patents related to these categories of arms (art. 7) and, at the same time, limit the orders for the home trade.

According to the general conditions of the contract (*Cahier des charges generales*), agreements on the manufacture of war material require permanent supervision of the manufacturing process. The administration is entitled not only to the general right of supervision but also to the right of unilateral modification of the contract.[22]

---

[22] A. de Laubadere, 2 *Traite theorique et pratique des contracts administratifs* 410-411 (Paris, 1956).

GREECE

PERSONNEL INTEGRITY UNDER GREEK LAW

Prepared by Theresa Papademetriou
Senior Legal Specialist
European Law Division
Law Library, Library of Congress
January 1985

I. Background

Verification of public employees' allegiance and loyalty to the political regime established by the Constitution has had a long history in Greece and has gone through various stages.

At the end of the civil war, under Law 516/1948[1] and a series of regulations, a rather strict verification of loyalty was initiated for public employees and employees of various enterprises that were subsidized directly or indirectly by the Government. Verification was limited not only to employees' current beliefs and ideals but was also extended to their past activities. Initially, it was done at the time the employee was appointed, but it could take place anytime during the course of employment.

During the dictatorship of 1967-1974, the Government took more drastic measures in an effort to secure its position and verify employees' loyalty. It set a time limit of six months, during which the loyalty and devotion of public employees was tested. All employees had to disclose information on their personal and family status and answer in great detail numerous questions such as whether they ever had had contact with a member of the Communist party; or had ever participated in a political gathering in which the public order and safety were endangered; or had admitted that the Communist party through its actions had betrayed the national interests and attempted to overthrow the regime, seize power, and subjugate the country under the communist regime; or whether they had promised they would abstain from any acts against the State; etc. Finally, they had to submit a statement by which they declared and reaffirmed their devotion to the Government.[2] This verification together with Laws 4 and 19 of 1967, as amended by Law 65/1967,[3] led to the firing of a number of public employees for various acts that were incompatible with their duties and capacity as public employees.

---

[1] P. Raptarchis, 2B Diarkes Kodix Nomothesias (Continuous Compilation of Laws, hereafter cited as Raptarchis) 431(d). (Looseleaf)

[2] N. Alivizatos, Oi Politikoi Thesmoi Se Krise 1922-1974 Opseis Tes Ellenikes Empeirias (Political Institutions in Crisis, 1922-1974; Some Aspects of the Greek Experience) 616 (Athens, 1983).

[3] Raptarchis, at 452,01(j).

The definition of "loyalty" had a very specific interpretation at that time. An unloyal employee was a person who was a communist or had anti-national ideas, made propaganda in favor of these ideas, or committed acts against the existing political regime, participated in a riot or in a forbidden public gathering in which the participants shouted communist slogans, etc.

The situation described above reflects the political turmoil and instability that Greece experienced from the end of World War II to the collapse of the dictatorship in 1974.

II. 1974 to the Present Time

After the smooth transition in 1974-1975 from a dictatorship to a democracy, the verification of employees' loyalty and devotion to the democratic regime of the country was limited only to employees who applied to those ministries and services whose area of jurisdiction refers to national defense, public order, and safety or those areas that are of an absolutely confidential nature. For all other public employees, a good moral character and healthy socio-political ideas are sufficient according to Presidential Decree 611/1977 on Codification of All Provisions in Force Pertinent to the Status of Public Employees and Employees of Legal Entities of Public Law.[4]

Presidential Decree 410/1975[5] determines the type and contents of the certification that must be completed by those applicants who are appointed as public employees in the Ministry of National Defense and in services whose jurisdiction is related to national defense.

The scope of activities of the Government Information Service (Kratike Yeperesia Pleroforion, KYP) includes the collection of information related to national defense, the monitoring of activities of members of the Communist party should they be against the established political regime, and the monitoring of any foreign spy missions.[6] In regard to this Service, Presidential Decree 966/1976[7] states that the type and contents of certification of those who apply are the same as determined by Presidential Decree 410/1975 and are completed by applicants of the Ministry of National Defense.

---

[4] Raptarchis, 2A at 316,713(d).

[5] *Id*. 36, at 60,213.

[6] Under Law 1415/1984 monitoring of activities of members of the Communist Party by KYP is terminated.

[7] Raptarchis, at 62,09(a).

The first part of this certification includes general questions on the personal status of the applicant, such as nationality, profession, address, etc. It also includes questions about the families of the applicant's father and spouse. All information provided is in lieu of a curriculum vitae and is kept in the personal file of the employee; it is kept absolutely confidential. The second part of the certification is composed of a questionnaire. A literal translation of this questionnaire is appended.

Appendix

QUESTIONNAIRE

(Second Part of Certification)

1. Have you ever been accused or convicted? By what court? For what reasons and to what type of punishment?
2. Have you ever traveled abroad? If yes, where, when, and for what reason? How long? (Tourism - scientific purposes - scholarship - studies - medical treatment - commercial purposes - conventions, etc.)
3. Have you ever belonged or do you currently belong to a domestic or foreign organization? Which one? As an ordinary member or as one having authority?
4. When and how did you become a member of such an organization? Are you still a member? If you have been dropped (from membership), when and why?
5. Do you renounce any kind of organization, party, or doctrine that aims to overthrow the constitutional regime of the country by violent means?
6. Will you obey the orders of the lawful government if there is a need to resist forcefully those who develop subversive activities?
7. Are you devoted to the legal regime of the country as established by the Constitution?
8. Have you ever been involved in situations that were against the nation, regime, or national security? If yes, when and how specifically?
9. Have you ever used a different last name or a pseudonym? If yes, when, in what case, and why?

10 To the best of your knowledge, has any member of your immediate family or the family of your father or of your spouse's father ever been a member or currently is a member of an organization? If yes, which one? When and how did that person become a member? If dropped (from membership), when and why? What position did that person have in the organization or does he now have? Have you ever cooperated with this person?

11 To the best of your knowledge, have any of the persons mentioned in question 10 been executed, imprisoned, convicted or expelled? If yes, by whom, for what reason?

12 Do you promise that you will never reveal official secrets or other information brought to your attention through your position?

I certify,

knowing the legal consequences on the personal responsibility of the declared, that the above statement is true and complete, and I have not kept secret any information related to all of the above questions.

Date and Signature

ITALY

Prepared by Dr. Giovanni Salvo
Senior Legal Specialist
European Law Division
Law Library, Library of Congress
September 1984

On the basis of current legislation in Italy, anyone who meets certain requirements can establish a work relationship with a public agency. Common requirements include Italian citizenship, physical fitness, a minimum age, the possession of civil and political rights, and proper moral conduct.

Furthermore, Law No. 15 of January 4, 1968, establishes that the possession of various requirements can be proven with a statement signed by the interested party in substitution of the official documents. The agency may later request the official documents. Good conduct and the absence of a criminal record and pending charges, when required, are verified directly by the interested agency through the appropriate public offices.

Articles 355 and 356 of the Italian Criminal Code contain provisions on breach of public supply contracts and fraud in public supply which apply to suppliers of the Public Administration. The pertinent articles of the Criminal Code, in an English translation, are included as an Appendix.

THE ITALIAN PENAL CODE

Article 355. Breach of Public Supply Contracts.

> Whoever, through non-performance of the obligations arising under a contract of supply concluded with the State, or with another public body, or with an enterprise performing public services or services of public necessity, causes a shortage, in whole or in part, of goods or services which are necessary to a public establishment or public service, shall be punished by imprisonment for from six months to three years and by a fine of not less than 40,000 lire.
>
> The punishment shall be increased if the contract relates to:
>
> (1) food or medical supplies, or goods or services to be used for land, water, air, telegraph or telephone communications.
>
> (2) goods or services to be used for the armament or equipment of the armed forces of the State; or
>
> (3) goods or services to be used to obviate a common danger or public disaster.

If the act was committed by negligence, imprisonment for up to one year, or a fine of 20,000 to 800,000 lire, shall be imposed.

The same provisions shall apply to subcontractors, brokers and agents of the supplier, when they, by breaching their contractual obligations have caused the shortage of supplies.

Article 356. Fraud in Public Supply.

Whoever commits fraud in the performance of a contract of supply or in the performance of the other contractual obligations specified in the preceding Article shall be punished by imprisonment for from one to five years and by a fine of not less than 400,000 lire.

The punishment shall be increased in the cases designated in the second paragraph of the preceding Article.

#

THE NETHERLANDS

Prepared by Dr. Karel Wennink
Legal Specialist
European Law Division
Law Library, Library of Congress
September 1984

The status of civil servants in the Netherlands is based on the Law on Civil Servants[1] and is further regulated by the appropriate authorities in the General Regulation on Civil Servants.[2]

The appointment to a position for a period of longer than 3 months can only be effective, if it is based on an inquiry into the individual's personal history and no objection exists against the person concerned.[3]

The rules concerning the inquiry into the individual's personal history have been established by decree.[4] If a position of trust is involved, a special security inquiry has to be made after it has been determined that no objection based on the inquiry into the records of the person concerned exists.[5] The individual is informed by the appropriate authorities at the start of the security inquiry.[6] Rules concerning this security inquiry have also been established by decree.[7]

If, based on the results of the security inquiry, the appropriate authorities have doubts whether or not the investigated person can fulfill, under all circumstances, his duty as a civil servant or employee so that it is assumed that for that reason he cannot be considered suitable for the position, the individual must be notified in writing. The objections are mentioned in this notification. Within 8 days after the reception of this decision the person can submit his notice of appeal, and a special advisory committee is asked to give an opinion.[8] The committee meets between 2 and 3 weeks after reception of the appeal. The committee can do its own investigation in order to get all the information which it thinks will be needed in order to give advice. The person investigated is informed of the time and place of the meeting of the committee so that he can be heard. The individual may appear either with or without an adviser. After the committee has formed an opinion, it is immediately related to the appropriate authorities.[9] If the authorities, after having received the advice, determine that the person concerned cannot fulfill the position of trust, they immediately notify the person in writing. The individual must be informed of:

---

[1] Law of December 12, 1929, Staatsblad (official law gazette of the Netherlands, Stb.) 530, as amended.
[2] Decree of June 12, 1931, Stb. 248, as amended.
[3] *Id.* art. 8.
[4] Decree of October 14, 1969, Staatscourant (official daily paper of the Netherlands, Stcrt.) 209.
[5] *Id.* art. 1, para. c; art. 2, para. 1.
[6] *Id.* art. 2, para. 2.
[7] Decree of May 10, 1976, Stcrt. 167.
[8] *Id.* art. 5.

a) the reasons which lead to the decision, without revealing the source of the information; and

b) whether or not the decision is in agreement with the advice from the committee.[10]

---

[9] *Id.* art. 6.
[10] *Id.* art. 7.

SECURITY CLEARANCES IN THE BRITISH CIVIL SERVICE

Prepared by Kersi B. Shroff
Senior Legal Specialist
American-British Law Division
Law Library, Library of Congress
December 1984

Since the 1950's, Britain has operated a formal system of granting security clearances to its civil service personnel involved in gathering intelligence, providing security and serving in other sensitive occupations. The system known as "positive vetting" at present covers nearly 66,000 civil servants and some employees of defense contractors. The system was started under the government of Winston Churchill in 1952, although it was accepted in principle by the previous government of Clement Attlee, as a result of intense American pressure applied after the conviction of Klaus Fuchs for passing atomic secrets.[1]

Details concerning the steps undertaken during positive vetting are not available,[2] but an outline is obtainable from two investigative reports issued by the Security Commission in recent cases in which serious security lapses have occurred in the country.[3]

Positive vetting clearance is granted after extensive interviews with two character references (referees) whose names have been supplied by the subject whose background is being investigated. If the referees are not available or have not had sufficient contact with the subject in the previous five years, two alternate referees are appointed. Positive vetting is carried out prior to appointment and then after every five years. A clearance is also required if there is a change in personal circumstances, for example on marriage. In special cases, positive vetting is carried out on an annual basis.

---

[1] The Times (London), April 16, 1984, at 12. Until 1965, positive vetting clearance was required only for staff with access to "Top Secret" material. Since then the clearance is required from all staff with access to any intelligence material.

[2] In the case of the armed forces, the Ministry of Defense (MOD) issues general security regulations in a manual known as 'MOD Manual 4.' The manual does not appear to be publicly available.

[3] Gt. Brit., Prime Minister, Report of the Security Commission March 1984, Cmd. 5, No. 9212 (1984); Gt. Brit., Prime Minister, Report of the Security Commission May 1983, Cmd. 5, No. 8876 (1983). (Copies of both reports are attached.) The Security Commission conducts inquests on cases involving serious breaches in security and reports directly to the Prime Minister. (See the detailed chart on "Whitehall's Anti-Spy Machine" in The Times (London), April 16, 1984, at 12. A copy is attached. Note also the Personnel Security Committee, a Civil Service group supervising the positive vetting system.)

The investigation is carried out by Positive Vetting Investigation Officers (PVIO), all of whom have several years of experience in investigations prior to appointment. PVIO are also given in-house training.

As a result of the inquiry by the Securities Commission in the cases of two personnel involved in espionage (Philip Aldridge convicted for attempting to communicate a highly classified document to the Russian Intelligence Service and Geoffrey Prime, convicted for spying for the Russians from 1968 to 1981 while employed at the highly sensitive Government Communications Head Quarters (GCHQ)),[4] several recommendations were made for the improvement of the positive vetting system. The proposals set out in the appendices to the reports, however, are deleted from the published verions of the reports, on account of the classified information contained in them.[5] Some other proposals for the improvement of the system have been published. They are:

1) The decision to grant or withhold a positive vetting clearance should be taken, in a case of material doubt, by an officer of Assistant-Secretary grade or above.

2) The PVIO should report formally on the subject's motivation at initial positive vetting.

3) Additional staff should be hired to clear the backlog of interviews for positive vetting reviews.

4) All personnel in the securities and intelligence agencies should be given polygraph examinations.

5) The same personnel should undergo psychological tests.

Additionally, a far more searching method of "neighborhood inquiries" into the background of subjects has also been introduced.[6] In a related development, the House of Lords, Britain's highest court, recently upheld the right of the government to ban trade union membership by the staff of GCHQ.[7] The ban is justified on grounds of national security.

---

[4] GCHQ is linked to the United States, Australia and New Zealand in sharing intelligence information. The existence of GCHQ was not generally known until May 1983 when the Prime case "blew its cover."

[5] The reports cited, supra note 4, copies of which are attached, make interesting reading on intelligence procedures.

[6] The Times (London), April 16, 1984, at 12.

[7] R. v. Secty of State for the Foreign and Commonwealth Office and Another, Ex parte the Council of Civil Service Unions and Others, The Times (London), Nov. 23, 1984, at 23.

Although the Security Commission report in the case of Geoffrey Prime could find no fault in those responsible for the operation of the positive vetting system, it has been stated that "everyone, including the security commission, knows that it is a shambles, with overworked, out-of-touch investigation officers struggling to keep up."[8] The Cabinet Office has carried out a review of the positive vetting procedures, details of which are not made public. It is evident that the changes which have already been introduced in the system, e.g. polygraph and psychological tests, have resulted from the great concern expressed by the American government over the lapse revealed by the case of Geoffrey Prime. It is acknowledged that if the United States were to withdraw its partnership with Britain in intelligence matters, an important asset would be jeopardized as Britain itself could not maintain a worldwide intelligence gathering capability on an independent basis. Whether the changes in the system will ensure that cases such as that of Geoffrey Prime will not occur in the future remains to be seen. The Times (London) is not sure that further security scandals will not be uncovered:

> Counter-intelligence professionals always preface any remark with a warning that no system is watertight; that the KGB continues to devote immense resources to penetrating the British intelligence establishment and are very good at it .... Mrs. Thatcher is the fourth prime minister since 1945 to have been prodded by scandal into spinning a finer mesh for the anti-spy net.
>
> .... The Prime affair persuaded Mrs. Thatcher to follow where Attlee, Eden and Macmillan had led. It would be reassuring to think that her improvements had, at long last, put the Whitehall spy catchers ahead of the KGB controllers. But life in the espionage branch of the cold war business is not as simple as that.
>
> For a variety of reasons--ideological, psychological, or entrapment by sex and/or money--there could well be a network of Chernenko's Englishmen even among the 60,000 or so crown servants who pass through the positive vetting system.[9]

---

[8] The Economist, August 11, 1984, at 50 (U.S. edition).

[9] The Times (London), April 16, 1984, at 12. For a knowledgeable account of "Stalin's Englishmen" see C. Pincher, Their Trade is Treachery (1981).

SECURITY CLEARANCE OF CIVIL SERVANTS IN TURKEY

Prepared by Belma Bayar
Legal Specialist
Near Eastern and African Law Division
Law Library, Library of Congress
February 1985

The government of Turkey restricts civil service employment to Turkish citizens who must be of good character and loyal to the Turkish Republic.[1]

Thus, Article 48 of the Government Employees Act states that the government cannot employ persons who have been convicted of criminal acts with a jail sentence of more than six months or of any crime against the state.[2] Those eligible for public service must submit their financial disclosure statements when they enter the service and whenever asked during their employment. Furthermore, civil servants cannot engage in commercial activities or join political parties.[3]

Some government positions may require more restrictions because of their sensitive nature. For example, judges and police officers cannot marry foreigners, and foreign service employees must ask the permission of their department before they marry.[4] However, no laws or published regulations govern investigation procedures followed to investigate for prospective employees in sensitive positions.

The National Intelligence Service is responsible for the gathering of all information necessary for national security and for protecting government information, the passing of which would be damaging to national security.[5] According to the information received from the Turkish Embassy, the Intelligence Service conducts investigations of public officials in sensitive positions. The Prime Minister's Office determines the investigation procedure, which, however, cannot be disclosed because of its classified nature.

---

[1] Article 6 of Law No. 657 of July 14, 1965, in Fahri Coker and Sadi Kazanci, ed., Turkiye Comhuriyeti Kanunlari, p. 7502.

[2] Id. at 7512.

[3] Articles 7, 14 & 28, supra note 1, at 7502-7503.

[4] Article 7 of Law No. 1154 of June 25, 1927, as amended, supra note 1, at 1161.

[5] Article 4 of Law No. 2937 of November 1, 1983, in T. C. Resmi Gazete (Official Gazette of Turkey) No. 18210 of November 3, 1983, p. 8.

EXHIBIT NO. 6

Congressional Research Service
The Library of Congress

Washington, D.C. 20540

PERSONNEL SECURITY INVESTIGATIONS AND NATIONAL SECURITY: SELECTED REFERENCES

This bibliography's principal focus is:

- Personnel suitability for secure and sensitive positions;
- Background investigations;
- Security clearances; and
- Discovery of potential defectors

Related issues covered in an illustrative manner are:

- Classification of materials;
- Foreign intelligence services;
- Rules for the classification of materials;
- Foreign intelligence services operating in the United States; and
- Evaluations of the U.S. intelligence community's ability to prevent and detect counter-intelligence activities in this country

Most of the citations are annotated and have been chosen from the computerized bibliographic data base created and maintained by the Library Services Division of the Congressional Research Service. A number of citations were selected from the card catalog and the computerized catalog to the collections of the Library of Congress. The Public Affairs Information Service index was also consulted to assure a broad coverage of the subject area.

The author would like to thank Mark Lowenthal, Specialist in Foreign Affairs and National Defense, Fred Kaiser, Specialist in American National Government, Kent Ronhovde, Legislative Attorney and Section Head in the American Law Division, and Richard Gigax, Head of the Subject Specialization Section, Library Services Division, for their review of this work and their comments. The author would also like to thank Barbara A. Hall for the secretarial production of this bibliography.

Sherry B. Shapiro
Senior Bibliographer, Foreign Affairs
Library Services Division
June 4, 1985

Personnel Security Investigations and National Security: Selected References

The Accuracy and utility of polygraph testing. Polygraph, v. 13, Mar. 1984: whole issue.

Report of "a working group of senior examiners from the military services . . . setting forth the basis upon which the polygraph is utilized in the Department of Defense."

Beichman, Arnold. Can counterintelligence come in from the cold? Policy review, no. 15, winter 1981: 93-101.

A pessimistic view of the future for U.S. intelligence and counter-intelligence.

Boyle, Andrew. Britain's establishment spies. New York times magazine, Dec. 9, 1979: 58-60, 62, 64-66, 128, 130-133.

"What was it that drew these men of privilege and talent to espionage and treason? In [this] excerpt from 'The Fourth Man,' Andrew Boyle seeks an explanation."

Bullough, Vern L. How I became a security risk. Nation, v. 222, Feb. 7, 1976: 140-142.

Criticizes procedures and motives of personnel investigations conducted by intelligence-internal security agencies, based on evaluation of the author's own dossier compiled by naval intelligence in the 1950's and obtained under the Freedom of Information Act.

The C.I.A. & the 'rogue agents'. Nation, v. 233, Nov. 28, 1981: 561, 563-571.

Partial contents.--The Wilson-Terpil case.--The Chilean connection, by S. Landau and J. Dinges.

Crapnell, Stephen G. Security clearance delays cost government, industry millions. Occupational hazards, v. 44, May 1982: 33-36.

The author considers "losses caused by the Federal government's delays in processing security clearances for DoD and contractor personnel. On the basis of an estimated 130,000 clearance requests from industry in 1982, these processing delays could cost industry and government about $340 million this year."

Crawford, James. Security clearance procedures called 'hodge podge.' Federal times, Apr. 29, 1985: 3, 16.

"Too many unnecessary clearances are provided, leaving insufficient resources where investigations are warranted. . . . Many employees hold clearances based on 20-year-old information, despite a requirement that they be re-investigated every five years."

Donner, Frank. How J. Edgar Hoover created his intelligence powers. Civil liberties review, v. 3, Feb.-Mar. 1977: 34-51.

Explores Presidential documents, departmental regulations, and statutes to discover the origins and legitimacy of the FBI's authority to conduct political intelligence operations, concluding "that the bureau's intelligence powers are . . . the result of an intelligence coup, a mission which succeeded for 30 years."

Ehlke, Richard. Political surveillance and police intelligence gathering --rights, wrongs, and remedies. Wisconsin law review, v. 1972, no. 1, 1972: 175-199.

Comment considers Anderson v. Sills, which challenges the constitutionality of "current police practices of collecting and maintaining intelligence information."

----- Polygraphs, secrecy, agreements and the protection of national security information. Federal Bar news & journal, v. 31, Mar. 1984: 96, 131.

"The Reagan Administration has made several significant initiatives to prevent what it sees as damaging disclosures of national security information. Soon after it assumed office, it began a reevaluation of the standards governing the classification of national security information. This review resulted in a new Executive Order (E.O. 12356). . . . It issued National Security Decision Directive--84 on Safeguarding National Security Information (NSDD-84). The Directive called for increased use of polygraph examinations in leak investigations and secrecy agreements to be signed by persons with access to classified information."

Epstein, Edward Jay. Edwin Wilson and the CIA: how badly one man hurt our Nation. Parade magazine (Boston globe), Sept. 18, 1983: 22, 24-25.

----- The war of the moles. New York, v. 11, Feb. 27, 1978: 28-38; Mar. 6: 55-59.

Author of a book about accused assassin Lee Harvey Oswald is interviewed about Oswald's relations with the Soviet KGB and an alleged connection between Oswald's reputed activities and the suspected presence of Soviet-controlled "moles"--double agents--burrowing into the CIA and FBI.

----- The war within the CIA. Commentary, v. 66, Aug. 1978: 35-39.

Examines leaks of CIA information and considers why such leaks occur.

Ervin, Sam J., Jr. Privacy and government investigations. University of Illinois law forum, v. 1971, 1971: 137-153.

"A quiet America will not be a free America. Rather, it will be a spiritually lifeless America. For that reason I believe that this claim of an inherent executive branch power of investigation and surveillance on the basis of people's beliefs and attitudes may be more of a threat to our internal security than any enemies beyond our borders."

Felling, Richard L. Multidiscipline hostile intelligence service threat. Military intelligence, v. 7, Oct.-Dec. 1981: 12-15.

"The Army's Counterintelligence Production Division of the Intelligence and Threat Analysis Center (ITAC) views the threat from the hostile intelligence services as an integrated, well-coordinated, all-encompassing onslaught of intelligence and special operations activities."

Gallagher, Michael G. Defense of adverse actions against Federal civilian employees occasioned by the revocation of a security clearance. Army lawyer, no. 126, June 1983: 18-30.

"It is the purpose of this article to present general guidance in representing the agency [Dept. of the Army] before the [Merit Systems Protection] Board. Specific emphasis is placed upon defending agency adverse actions which are occasioned by the revocation of a security clearance."

Gash, Norman. Over there: a scholar and a traitor. Policy review, no. 15, winter 1981: 153-160.

A look into extent of Soviet penetration of the British diplomatic and intelligence services: the case of Sir Anthony Blunt.

Goldberg, Jeff. Who killed John Paisley? Inquiry (San Francisco), v. 2, Oct. 15, 1979: 11-16.

"The CIA calls his death a suicide, but the evidence suggests that the former intelligence analyst was another casualty in the war over the Russian 'mole' inside the CIA."

Handleman, Howard. The Soviet KGB in America. Air Force magazine, v. 62, June 1979: 57-60.

"The number of Soviet spies in America has increased significantly in recent years, raising concern about the ability of US counterintelligence to cope."

Hanrahan, John D. Foreign agents in our midst. Progressive, v. 41, Nov. 1977: 31-35.

Focuses on U.S. activities of the intelligence agencies of Chile, Iran, and South Korea.

Hurt, Henry. CIA in crisis: the Kampiles case. Reader's digest, v. 114, June 1979: 65-72.

Kampiles, a former CIA employee sold a technical manual of strategic importance to the Soviet Union. The article raises some disturbing questions about the national security and the need for an effective intelligence service.

Jacobs, Arthur L. Foreign intelligence ethics of the craft. Freedom at issue, no. 66, May-June 1982: 6-8.

The author proposes "a Credo and a Code of Ethics for the intelligence craft and those who practice it. This code is not meant to be a substitute for their personal and individual ethics--but an addition to them."

Jaffe, Harry. The B-Team. Regardie's, v. 5, Dec. 1984: 78-80, 82, 84-86, 88.

Examines the workings of CIE (Counter Intelligence Espionage) Enterprises, Limited, a Washington-based firm of "private detectives with something extra"--expertise in government intelligence work applied to the business community.

Jameson, Donald. The clandestine battlefield: trenches and trends. Strategic review, v. 11, winter 1983: 19-28.

"Soviet and U.S. capabilites in the critical arena of intelligence and covert operations. . . . The most pronounced Soviet edge lies in the area of covert action--an area in which, moreover, the United States still labors under self-inflicted damage."

The KGB's spies in America. Newsweek, v. 98, Nov. 23, 1981: 50-54, 61.

Analyzes the KGB's mission, methods and impact, and assesses the challenge it poses to the open society of the U.S.

[Laws, etc.] Compilation of intelligence laws and related laws and Executive orders of interest to the National Intelligence community. Prepared for the use of the Permanent Select Committee on Intelligence of the House of Representatives. Washington, G.P.O., 1983. 351 p.

At head of title: 98th Congress, 1st session. Committee print.

LaVoy, Diane Edwards. Foreign nationals and American law. Society, v. 15, Nov.-Dec. 1977: 58-64.

"The ability of an open society to protect itself from foreign manipulation is limited."

Ledeen, Michael. A mole in our midst? New York, v. 11, Oct. 2, 1978: 55-57.

"Intelligence analysts, including more than one ex-CIA chief, say a foreign agent may have penetrated the administration."

Levchenko, Stanislav. [KGB activities and peace movements: an interview with KGB defector Stanislav Levchenko] In Remarks of William L. Armstrong. Congressional record [daily ed.] v. 129, Apr. 12, 1983: S4447-S4450.

This interview originally appeared in the West German periodical Der Spiegel on February 14, 1983. Levchenko, who was a KGB agent in Japan from 1975 until his defection to the West in 1979, describes KGB activities, including actions to infiltrate political groups and the news media.

Lewy, Guenter. Can Democracy keep secrets? Policy review, no. 26, fall 1983: 17-29.

Contends that "the United States may be the only nation . . . without any meaningful defense against the publication of classified defense information."

----- The Federal loyalty-security program: the need for reform. Washington, American Enterprise Institute for Public Policy Research, 1983. 90 p. (AEI studies 376)

"Legal and political problems have developed since the 1960s that seriously inhibit the effectiveness of the federal loyalty-security program. The author argues that key provisions of the present personnel security program, now almost thirty years old, are badly outdated: they sweep too broadly, yet no longer ensure the loyalty and trustworthiness of officials in truly sensitive positions. The government should abandon the pretense of an all-encompassing loyalty program . . . and should limit screening measures to positions that involve access to classified information or the ability to make or influence policy."

Lindsey, Robert. To be young, rich--and a spy. New York times magazine, May 22, 1977: 18, 89, 91-92, 94, 106, 108.

"Two young men from one of America's most privileged suburban communities had penetrated one of the most secret intelligence-gathering operations of the C.I.A., and for almost two years had been sending a river of secrets to Moscow."

Lynch, Mark H. Secrecy agreements and national security. Government information quarterly, v. 1, no. 2, 1984: 139-156.

In the spring of 1983, President Reagan issued a National Security Decision Directive which, among other provisions, mandated that present and future Executive Branch employees and contractors having access to classified information or sensitive compartmented information, the latter being a kind of intelligence data, sign one of two types of nondisclosure agreement. Previously, these types of agreements had been used for the most part only in the intelligence agencies. This article reviews the law which has developed around the prepublication review requirement of Central Intelligence Agency agreements and examines the contracts mandated by the new National Security Decision Directive, identifying issues raised by these agreements in light of the body of case law dealing with the C.I.A.'s system of censorship. With regard to the prepublication review requirement, the focus here is limited to former rather than current officials of the government.

Martin, David. How to keep Soviet moles out of government. Human events, v. 43, Aug. 20, 1983: 9-14.

"Since the collapse of U.S. internal security in the early 1970s, the United States has again become vulnerable to penetration by Americans recruited by Moscow and Havana. David Martin, noted security expert, discusses penetration in the past by such notorious agents as Alger Hiss and Harry Dexter White and outlines a remedy to prevent a reoccurrence of further political and intelligence disasters."

----- Putting secret puzzles together. Washingtonian, v. 18, Mar. 1983: 89-92, 94-95.

"Authors such as James Bamford and Anthony Cave Brown are mining declassified documents for best-sellers. . . . Their success has not only upset some of the government's secret-keepers, it has led the Reagan administration to reconsider its handling of sensitive information, and even to attempt to get some material now in the public domain back under wraps."

----- Screening Federal employees: a neglected security priority. [Washington] Heritage Foundation [1983] 103 p.

"Critical issues"

Examines the present "U.S. security weakness" and recommends "completely revising the current lax guidelines for adjudicators and investigators; and reactivating the FBI's domestic intelligence division and the Security Research and Analysis Section at the Office of Personnel Management."

Murphy, Charles J. V. Uncloaking the CIA. Fortune, v. 91, June 1975: 88-91, 197, 199-200, 202-204.

"No intelligence agency can do its job effectively unless it can keep its operations secret. That's why the investigative hysteria in Washington is so dangerous for U.S. security.

Newton, Verne. The spy who came to dinner. Washingtonian, v. 20, Oct. 1984: 95-96, 100-102, 104-108.
"It was 1951 and no one suspected that Kim Philby was a Soviet spy. But an incident at a Washington dinner party would begin to change all that."

Oglesby, Carl. The man who came in from the cold. Maybe. Boston magazine, v. 71, Oct. 1979: 45-48, 51-52, 54, 56-59.
Reviews the case of former Soviet intelligence officer Yuri Nosenko, who told the CIA after his 1964 defection that accused Kennedy assassin Lee Harvey Oswald was not operating under KGB instructions. "Sharp changes in Nosenko's fortunes with the CIA define the main twists of a spy story that has become basic to our understanding of the JFK assassination, the conflict within the CIA, the apparent murder a year ago of a covert CIA officer named John Paisley, and the still unfolding drama of alleged Soviet moles in the top levels of the CIA."

Osborne, David. Japan's secret agents. New republic, v. 191, Oct. 1, 1984: 20-23.
Reveals how officials and experts in the Office of the United States Trade Representative and other agencies involved in international trade matters frequently become lobbyists, lawyers, and consultants for Japanese interests when they re-enter private life. "The wide-open way we do business in Washington may suit American industry just fine. . . . But it suits our economic competitors even better."

Otte, Monica A. Aliens in the Federal civil service. Cornell international law journal, v. 10, May 1977: 255-279.
Analyzes "the various national interests which have been advanced in support of the exclusion."

Plugging leaks. New York, WNET/Thirteen, 1983. 8 p.
The MacNeil-Lehrer Report, April 29, 1983.
Attorney Floyd Abrams, deputy assistant attorney general Richard Willard, former CIA general counsel Daniel Silver, and journalist and former State Department assistant secretary for public affairs Hodding Carter discuss the Reagan Administration's Mar. 1983 "stop the leaks" directive requiring a secrecy pledge, submission to polygraph examination, and lifetime prepublication clearance for all Government employees with security clearances.

Scientific validity of polygraph testing: a research review and evaluation. Washington, Office of Technology Assessment, for sale by the Supt. of Docs., G.P.O., 1983. 132 p.
Discusses "the various types of polygraph testing procedures and ways in which the polygraph is used, and then summarize[s] the judicial, legislative, and scientific controversy over polygraph testing validity."

Southerland, Daniel. Spy wars. Christian Science monitor, Sept. 22, 1980: 1, 12-14; Sept. 23: 11-14; Sept. 24: 11-14; Sept. 25: 11-14; Sept. 26: 11-14; Sept. 29: 1, 14-16.
Contents.--The global struggle for power.--KGB: the Soviet Union's principal intelligence agency.--Paris copes with a new kind of spy.--Front lines of espionage.--The Mideast: how the West was wrong.--Can a democracy operate in secret?

Spex, Milt. How to steal Government secrets. Washington monthly, v. 10, Feb. 1979: 54-60.
Pseudononymous defense contractor sees the information security system weakened by "tribal frictions, sloppiness and cynicism" and calls for less classification of documents to produce "a security system whose members have a renewed faith that the secrets they are protecting really are secrets. That might encourage us to follow the rules without cutting our accustomed corners."

Spies: foot soldiers in an endless war. Time, v. 98, Oct. 11, 1971: 41-24, 44, 46, 48.

Spies in Washington. Washington post magazine, Dec. 4, 1983: 18-25, 34-41, 54-56, 60-61, 63, 66, 68-69.
Contents.--The Inman file, by J. Conaway.--Counterspy, by L. Meyer. --Hey Ivan, say 'cheese', by L. Meyer.--Searching for the spies of tomorrow, by L. Katz.--Big brother is listening, by J. Bamford.--Tell me more, tell me more, by B. Arnebeck.--Missions from Moscow, by D. Nossiter.--Smoke gets in your eyes, by G. Moore.--Spy rings of one, by G. Lardner.--The admiral's brief guide to American spying.

Stavins, Ralph L. Should whistle-blowers in national security agencies be protected? Center report, v. 9, Feb. 1975: 3-5, 28.
Recommends a "personal accountability bill for civil servants at the GS-15 level and above; an employee disclosure bill for those below; a special prosecutor's office attached to Congress to enforce both laws; and a sovereign public body to exercise oversight on the special prosecutor and congressional committees."

Stein, Jeffrey. Spy versus spy in Washington. Saturday review. v. 6, May 26, 1979: 13-16.
Discusses intelligence and internal security operations and agents in the Washington metropolitan area.

Szulc, Tad. I spy, you spy. Washingtonian, v. 14, Nov. 1978: 97-102, 104, 107.
"Today much of the deadly serious business of espionage is transacted in Washington. The city's government buildings, foreign embassies, newspaper offices, hotels, private dwellings, exclusive restaurants, shabby bars, and quiet public libraries are the scenes of endless and sometimes lethal intelligence games."

----- Inside South Korea's C.I.A. New York times magazine, Mar. 6, 1977: 41-42, 44, 46, 50.
Outlines the organization and activities of the KCIA, focusing on its alleged gifts to U.S. Congressmen and its intimidation of Korean residents in the U.S.

----- The KGB in Washington. Washington post magazine, Mar. 2, 1980: 12-18.
"There are about 200 Soviet agents here. They read a lot, attend congressional hearings, have lunch with the right people and, of course, they recruit infiltrators."

----- The missing C.I.A. man. New York times magazine, Jan. 7, 1979: 13, 15, 56, 60, 62.
"His 'suicide' was bizarre; the nature of his C.I.A. work, top-secret. Who was John Arthur Paisley, and what actually happened to him?"

----- The Shadrin affair: a double agent double-crossed. New York, v. 11, May 8, 1978: 42, 44-48.

"Shadrin disappeared after United States intelligence senselessly thrust him into the role of double agent with the KGB."

Teller, Edward. The secrecy charade. Reason, v. 14, Nov. 1982: 42-45.

"The goal of changes in our secrecy laws should be to bring about an even stricter policy on a level of less stringency--that is, better protection of far less classified information. Such a policy, by the very fact that it would try to keep fewer secrets, could be more effective in areas that really matter."

U.S. Congress. House. Committee on Armed Services. Federal Polygraph Limitations and Anti-Censorship Act of 1984; report to accompany H.R. 4681 including cost estimate of the Congressional Budget Office. Washington, G,P.O., 1984. 14 p. (Report, House, 98th Congress, 2nd session, no. 98-961, part 2)

----- Full committee consideration of H.R.4681, relating to the administration of polygraph examinations and prepublication review requirements by Federal agencies. Hearing, 98th Congress, 2nd session. Sept. 19, 1984. Washington, G.P.O., 1984. 19 p.

At head of title: H.A.S.C. no. 98-46.

U.S. Congress. House. Committee on Government Operations. The Administration's initiatives to expand polygraph use and impose lifelong censorship on thousands of Government employees; twenty-fifth report together with additional and dissenting views. Washington, G.P.O., 1983. 77 p. (Report, House, 98th Congress, 1st session, no. 98-578)

"Concerning the Administration's proposals to expand the use of and reliance on polygraph examinations, the Committee concludes that there is no scientifically acceptable evidence to support these changes and good reason to believe they will result in high error rates, thereby causing harm to many innocent people and our government. . . . With regard to the prepublication review requirement mandated in the President's Directive, the Committee concludes that this censorship poses a serious threat to freedom of speech and debate cherished in our nation."

----- Justice Department handling of cases involving classified data and claims of national security; second report together with additional views. Washington, G.P.O., 1979. 28 p. (Report, House, 98th Congress, 1st session, no. 96-280)

Partial contents.--CIA reporting of offenses to Department of Justice. --Department of Justice access for internal use to information held by CIA. --Deciding whether conducting an investigation or disclosing information in court proceedings will damage national security.--Procedures to minimize disclosure while permitting court proceedings.

----- Security classification policy and Executive Order 12356; twenty-ninth report. Washington, G.P.O., 1982. 49 p. Report, House, 97th Congress, 2nd session, no. 97-731)

"The major findings of the report center on the failure of the Reagan Administration to change security classification rules or to solicit advice at a meaningful time during the revision process. In addition, the report concludes that the Reagan Administration failed to identify clearly the problems with security classification rules that the new order was intended to solve. The Administration also failed to explain in a satisfactory manner the purpose of the changes that were made. Finally, the report finds that overclassification of information continues to be a serious problem and that the new Executive Order offers nothing that will address the overclassification problem."

----- The use of polygraphs and similar devices by Federal agencies; thirteenth report together with separate and dissenting views. Washington, G.P.O., 1976. 61 p. Report, House, 94th Congress, 2nd session, no. 94-795)

Recommends "that the use of polygraphs and similar devices be discontinued by all Government agencies for all purposes."

U.S. Congress. House. Committee on Post Office and Civil Service. Federal Polygraph Limitation and Anti-Censorship Act of 1984; a report to accompany H.R. 4681 including cost estimate of the Congressional Budget Office. Washington, G.P.O., 1984. 60 p. (Report, House, 98th Congress, 2nd session, no. 98-961, part 1)

U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Civil Service. Federal Polygraph Limitation and Anti-Censorship Act of 1984. Hearings, 98th Congress, 2nd session, on H.R. 4681. Feb. 29, 1984. Washington, G.P.O., 1984. 333 p.

"Serial no. 98-39"

U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Investigations. Federal personnel security background investigations. Hearing, 96th Congress, 2nd session. Mar. 25, 1980. Washington, G.P.O., 1980. 42 p.

"Serial no. 96-76"

This hearing focuses on "improvements the Office of Personnel Management expects to make in the background investigation program."

U.S. Congress. House. Committee on the Judiciary. Subcommittee on Civil and Constitutional Rights. Use of polygraph tests by the U.S. Department of Defense. Hearing, 97th Congress, 2nd session, Dec. 9, 1982. Washington, G.P.O., 1984. 58 p.

"Serial no. 110"

U.S. Congress. House. Permanent Select Committee on Intelligence. Subcommittee on Legislation. Espionage laws and leaks. Hearings, 96th Congress, 1st session. Jan. 24, 25, and 31, 1979. Washington, G.P.O., 1979. 280 p.

----- Security clearance procedures in the intelligence agencies; staff report. Washington, G.P.O., 1979. 34 p.

At head of title: Committee print.

U.S. Congress. House. Permanent Select Committee on Intelligence. Subcommittee on Oversight. Pre-employment security procedures of the intelligence agencies. Hearings, 96th Congress, 1st session. May 16-June 21, 1979. Washington, G.P.O., 1980. 213 p.

----- Security clearance procedures in the intelligence agencies; staff report, Washington, G.P.O., 1979. 34 p.
At head of title: Committee print.

U.S. Congress. Senate. Committee on Armed Services. Polygraphs for counter-intelligence purposes in the Department of Defense. Hearing, 98th Congress, 2nd session. Mar. 7, 1984. Washington, G.P.O., 1984. 101 p. (Hearing, Senate, 98th Congress, 2nd session, S. Hrg. 98-1081)

U.S. Congress. Senate. Committee on Governmental Affairs. National Security Decision Directive 84. Hearing, 98th Congress, 1st session. Sept. 13, 1983. Washington, G.P.O., 1984. 206 p. (Hearing, Senate, 98th Congress, 1st session, S. Hrg. 98-568)

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. The erosion of law enforcement intelligence and its impact on the public security; report. Washington, G.P.O., 1978. 179 p.
At head of title: 95th Congress, 2nd session. Committee print.
Partial content.--Is law enforcement intelligence legal? A summary of court rulings.--Factors contributing to the erosion: the Freedom of Information Act and the Privacy Act; impact of the Tax Reform Act of 1976. --Consequences of the erosion: the crippling of abilities to deal with terrorism and civil disturbances; the weakening of the war against drugs; the impact on corporate and public security; the dismantling of the Federal employee security program.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Security and Terrorism. Communist bloc intelligence gathering activities on Capitol Hill. Hearing, 97th Congress, 2nd session, on S. 1959 and S. 1963. May 12, 1982. Washington, G.P.O., 1982. 67 p.
"Serial no. J-97-116"
This hearing addresses a request by the General Services Administration to dispose of Civil Service Commission personnel security investigative files for the years 1928 to 1959. It includes a statement by David Martin, entitled, "The erosion of the Federal Employee Security Program: a critique," p. 49-138.

----- Government files: retention or destruction? Hearing, 97th Congress, 1st session, on the request from the General Services Administration that concurrence be given to the disposal of Civil Service Commission personnel security investigative files for the years 1928 to 1959. Oct. 5, 1981. Washington, G.P.O., 1982. 564 p.
"Serial no. J-97-64"

U.S. Congress. Senate. Select Committee on Intelligence. Activities of "friendly" foreign intelligence services in the United States: a case study. Washington, G.P.O., 1978. 24 p.
At head of title: 95th Congress, 2d session. Committee print.
"This report sets forth the results of a year-long investigation into the role of United States intelligence agencies with respect to alleged improprieties by the government, representatives and agents of South Korea in the United States. The Committee's investigation was conducted as a case study of the activities of 'friendly' intelligence services in the United States."

U.S. Congress. Senate. Select Committee on Intelligence. Subcommittee on Secrecy and Disclosure. National security secrets and the administration of justice; report together with additional views. Washington, G.P.O., 1978. 51 p.

At head of title: 95th Congress, 2nd session. Committee print.

Examines the difficulties of prosecuting information leak and espionage cases which would result in the disclosure of classified material.

U.S. General Accounting Office. Continuing problems in DOD's classification of national security information; report to the Congress by the Comptroller General of the United States. [Washington] 1979. 35 p.

"LCD-80-16, Oct. 26, 1979"

"Some individuals at DOD did not comply with the provisions of the 1978 Executive order and DOD's regulation on the classification of national security information. As a result, there was improper use of classification of information, and deficiencies in the marking of classified information. To correct these conditions, DOD should expand the training given to classifiers and improve its independent inspections of classification activities."

----- Costs of Federal personnel security investigations could and should be cut; report. [Washington] 1979. 42 p.

"FPCD-79-79, Aug. 31, 1979"

"This report discusses the extent of the personnel security investigation program in Federal agencies, factors bearing on consolidating these functions into a single agency, and improvements needed before consolidation is feasible. It also evaluates improvements and savings which have occurred or are possible without full consolidation."

----- The Department of Justice needs to address the problem of two personnel investigations being conducted on all Bureau of Prisons employees; report to the Attorney General. [Washington] 1982. 7 p.

"GAO/GGD-82-56, July 8, 1982"

"All positions within the Bureau of Prisons are classified as 'sensitive' which requires that all employees obtain security clearances. In this report, GAO expresses the view that not all of the Bureau's positions need to be classified as sensitive and calls upon the Department to streamline the investigative process for positions that should be so classified. Except for correctional officers, the Department of Justice concurred in the need to reexamine the security classification of the Bureau's positions. However, it did not indicate whether it would take any action to streamline the investigative process."

----- Faster processing of DOD personnel security clearance could avoid millions in losses; report to the Congress by the Comptroller General of the United States; [Washington] 1981. 19 p.

"GGD-81-105, Sept. 15, 1981"

"A significant increase in the number of security clearance requests for Department of Defense (DOD) and contractor personnel and delayed processing time have resulted in lost productivity costing millions and weakened national security."

----- Further improvements needed in Department of Defense oversight of special access (carve-out) contracts; report to the Secretary of Defense. [Washington, G.A.O.] 1983. 13 p.

"GAO/GGD-83-43, Feb. 18, 1983"

"Special access contracts, including carve-out contracts for which the Defense Investigative Service does not make security inspections, require special and costly measures to protect especially sensitive information. . . . This report recommends actions that the Department should take to improve oversight of special access contracts. The Department's comments and GAO's evaluation are included in a separate report supplement (GAO/GGD-83-43 (A)) because the Department marked the comments 'FOR OFFICIAL USE ONLY'."

----- Oversight of the Government's security classification program--some improvement still needed; report to the Congress by the Comptroller General of the United States. [Washington] 1980. 54 p.
"LCD-81-13, Dec. 16, 1980"

----- Personnel security investigations: inconsistent standards and procedures, Civil Service Commission. [Washington] 1974. 18 p.
"B-132376, Dec. 2, 1974"
Recommends that, due to extensive differences among executive agencies in the object, scope, and use of loyalty-security investigations, this function be centralized in two agencies, for one defense employment and one for civilian employment.

----- Proposals to resolve longstanding problems in investigations of Federal employees, Civil Service Commission; report to the Congress by the Comptroller General of the United States. [Washington] 1977. 83 p.
"FPCD-77-64, Dec. 16, 1977"
"Executive Order 10450 authorizes investigations of Federal personnel. It is out of date. Inherent weaknesses in the order, more recent laws, and court decisions have made it impossible for the Civil Service Commission to carry out its responsibilities. . . . Implementation of recommendations in this report would: clarify authority; provide clear criteria for determining the extent of investigations; [and] establish controls to protect the privacy of individuals."

The Unseen conflict--foreign espionage operations against the United States. [Washington] U.S. Federal Bureau of Investigation [1983] 10 p.
"For the most part . . . the conflict between American counterintelligence forces and hostile, foreign intelligence services remains 'unseen,' shrouded in secrecy. It is the purpose of this pamphlet to shed some light on the targets and strategies of hostile intelligence services."

Ward, Nathaniel P. Espionage and the forfeiture of diplomatic immunity. International lawyer, v. 11, fall 1977: 657-671.
"All diplomatic privileges are subject to abuse. When the sending State invokes immunity for espionage, an act outside of official functions . . . it has abused the privileges and immunities recognized by the law of nations and the receiving State, with attendant repercussions on the international plane."

Whatley, Frederick W. Reagan, national security, and the First Amendment: plugging leaks by shutting off the main. [Washington] Cato Institute, 1984. 18 p. (Policy analysis no. 37)
Objects to the lifetime prepublication review requirements proposed by the Reagan Administration in National Security Decision Directive 84.

EXHIBIT NO. 7

Office of Intelligence Policy and Review

Washington, D.C. 20530

May 1, 1984

MEMORANDUM FOR ROBERT C. McFARLANE
Assistant to the President for
National Security Affairs

Re: NSDD-84 Study of Federal Personnel Security Program

The National Security Decision Directive on Safeguarding National Security Information (NSDD-84) requested the Attorney General, in consultation with the Office of Personnel Management, to establish a group to study the federal personnel security program and recommend appropriate revisions in existing Executive Orders, regulations and guidelines. After consultation with OPM, the Department of Justice convened a group consisting of representatives of the Office of Personnel Management, Department of Defense, Department of Energy, Department of Treasury, and the Federal Bureau of Investigation. Although a few additional agencies, including CIA, were advised of the progress of the group and provided recommendations to the group, other affected agencies were not invited to participate in this initial stage because of our belief that more could be accomplished by a smaller group that would identify principal areas for further examination and solicit a broader range of comments at a later date.

Preliminary meetings have identified several fundamental policy issues relating to the Government's personnel security program. The guidance of the National Security Council is required on these issues at this time in order for the group to proceed in an expeditious and efficient manner. Without such guidance, this study, like so many of its predecessors, is doomed to failure. Once we have received direction on these fundamental questions, the study group will begin drafting proposals that will implement these decisions and identify more specific issues.

As a preliminary matter, it must be noted that NSDD-84 was issued in the Intelligence Community context. However, any changes to Executive Order 10450, "Security Requirements for Government Employment," will affect many agencies in the Executive Branch that are not part of that Community. Thus, a threshhold issue concerns whether the authority for making these fundamental policy decisions should be the Intelligence Community and the National Security Council structure -- the Senior Interagency Group (Intelligence) and its Interagency Group/Countermeasures -- which participated in the development of NSDD-84 or the Office of Management and Budget, which traditionally coordinates policy proposals that have Executive Branch-wide scope. We have elected to forward this options paper through the NSC/SIG(I) system because of the origins of the NSDD but have recognized the broader interests involved by providing a simultaneous copy to OMB for dissemination as it sees fit.

ISSUE I. - Scope of Study

Should the group established under NSDD-84 focus its efforts on security standards for (a) access to classified information, (b) employment in sensitive positions generally, or (c) suitability for employment generally, including a general requirement of loyalty to the United States?

The relevant statutes and Executive orders distinguish, but in an uneven way, between suitability for federal employment and access to classified information. Suitability for federal employment is determined by reviewing an individual's competence and ability to perform in a particular position based upon criteria such as education, experience, training, health, supervisory potential, and ability to work with others. On the other hand, access to national security information depends upon a determination that an individual will protect classified information from unauthorized disclosure based upon criteria such as loyalty to the United States, trustworthiness, integrity, discretion and reliability.

Obviously, there may be considerable overlap in the nature of the information that is used to make these two determinations. Heavy and repeated drug use, for example, is a suitability indicator since it may prevent a person from functioning properly on the job, but it is also a security concern since it may indicate a lack of respect for authority or potential for compromise or entrapment. This overlap is particularly acute with regard to "sensitive" positions that do not involve access to classified information but involve other responsibilities, such as fiduciary, health or public safety matters, that offer the potential for serious consequences if mishandled.

Under 5 U.S.C. 3301 and E.O. 10577, OPM is given responsibility for establishing standards for general suitability for federal employment. Under E.O. 10450, Federal departments or agencies are required to ensure that all persons employed by them are "reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States." To this end, each agency is responsible for establishing programs to "ensure that the employment and retention in employment of any civilian officer or employee . . . is clearly consistent with the interests of national security."

Executive Order 12356, "National Security Information," like its predecessors, requires that each agency determine the "trustworthiness" of persons given access to classified information. However, the DCI has authority to establish special access programs for information pertaining to intelligence activities.

Policy, judicial and bureaucratic developments over three decades have raised a serious question of whether the reference to "national security" in E.O. 10450 means to include only positions requiring:

- access to classified information;

or is intended also include positions that involve

- proximity to classified information, with or without actual access; and

- sensitive (law enforcement, medical, fiduciary) or other functions unrelated to such access;

or is intended to require general loyalty to the United States for all federal employment regardless of the nature of the functions the person is expected to perform if hired as a federal employee.

It is against this backdrop of confusion and uncertainty that NSDD-84 mandated a study of the "federal personnel security program," a term that, in its most commonly understood sense, springs from Executive Order 10450. Thus, a threshhold question as to the scope of the NSDD-84 effort is whether this group should address only civilian access to classified information, all access to classified information (including contractors and military), occupancy of any sensitive position, or loyalty of all Government employees regardless of position or access.

Agency Positions

All entities represented on the working group, except the Treasury Department, agree that the group should limit its deliberations as much as possible to positions involving access or proximity to classified information, including contractors and military personnel.

The Treasury Department believes that suitability for sensitive positions without access to classified information should also be addressed.

RECOMMENDATION

The NSDD-84 personnel security study group should focus on the standards, procedures and authorities relating to access or proximity to classified information by all Government employees, contractors and military personnel and address the federal employment suitability program, including sensitive positions with no access to classified information, only insofar as necessary to ensure that a clear and consistent distinction is maintained between the two areas.

____________________ Approved

____________________ Disapproved

ISSUE II. - Relation to E.O. 10450

Should Executive Order 10450, "Security Requirements for Government Employees", be replaced, revised or supplemented?

If, as recommended, the group is authorized to focus on access to classified information, the question then becomes how such an effort should relate to E.O. 10450 which establishes general security requirements for federal employment. Executive Order 10450 was promulgated on April 27, 1953. It established a federal employment screening program based upon certain security requirements, including loyalty to the United States. E.O. 10450 requires that federal civilian employee appointments be based upon a background investigation, the scope and intensity of which varies with the extent to which the position offers the occupant the opportunity to have an adverse effect on the "national security". "Security" considerations such as access to classified information continued to be an important factor in the screening process. However, the fundamental purpose of the Order was to deny federal employment to persons who did not meet its requirements regardless of whether the positions for which they were being considered required access to classified information or were considered sensitive for other reasons.

Judicial decisions over the years have narrowed the meaning of the term "national security" to include only positions directly concerned with protection from internal subversion and foreign aggression. At the same time, the Executive branch attempted to refine the screening process generally by dividing sensitive positions into those that are "critical-sensitive" and those that are "noncritical sensitive." These terms include a broad range of positions that require a high degree of trust, such as fiduciary or policymaking functions, but that have no "national security" implications as that term has come to be more narrowly understood and that may not necessarily involve access to classified information. As noted earlier, these evolutionary developments have served to blur and confuse the precise meaning and scope of the term "national security" in E.O. 10450.

The system for protecting classified information requires that access be limited to federal employees who have a demonstrated "need to know" and have been determined to be trustworthy. This system is a subset of the general requirements for public employment established by E.O. 10450. However, because of the ambiguities inherent in E.O. 10450 and the term "national security," the personnel security program established by that order and intended to eliminate disloyal individuals from Government employment has come to be confused with personnel security programs intended to deny access to classified information to federal employees who have not been determined to be trustworthy and have no official need to know. The inadequacy of E.O. 10450 as a basis for regulating access to classified information is illustrated by the fact that military personnel, who may require access to very sensitive classified information, are not mentioned in or governed by that Order.

Agency Positions

The members of the group agreed that E.O. 10450 should not be significantly altered insofar as it relates to generalized requirements for federal employment. On the other hand, the standards, considerations and processes for granting access to classified information as a part of that employment should be clarified and made uniform throughout the Government. This may be accomplished by a new Executive Order dealing solely with personnel security programs for federal employees, contractors and military personnel who require access to national security information. This course of action is consistent with the jurisdiction conferred on this group by NSDD-84 and also recognizes that access to classified information is a significant question addressed independently of federal employment.

RECOMMENDATION

That the federal personnel security study group draft a new Executive Order concerning access or proximity to classified information by all persons, modifying E.O. 10450 only insofar as necessary to make clear that this determination is distinguishable from the general requirements of E.O. 10450 regarding federal employment.

______________________ Approved

______________________ Disapproved

ISSUE III. - Investigative Standards Under A New Order

Should there be a basic prescribed level of coverage and scope in background investigations for all persons requiring access to the same types of classified information?

Investigative standards and practices differ among agencies, depending upon the status of the person being investigated and the nature of the information to which the person requires official access. For example, military and contractor personnel are not included under E.O. 10450, and there is a completely different set of criteria for access to Sensitive Compartmented Information as compared to access to Top Secret or Secret information.

Logically, all classes of persons, whether civilian, military or contractor, should meet the same basic investigative standards since they all are seeking access to the same national security information. In addition, the most rational basis for drawing distinctions between investigations for access to various categories of information is the sensitivity of that information as described in the E.O. 12356 classification system. That Executive Order provides for three levels of classification, Top Secret, Secret and Confidential, depending upon the gravity of the potential damage to the national security that might result from the information's unauthorized disclosure. That order also provides authority for establishing special access programs for especially sensitive classified data, such as Sensitive Compartmented Information.

The creation of basic investigative standards that are related to the sensitivity of the information to which access will be granted raises three problems. First, some agencies have been compelled in the past to reduce the scope and coverage of background investigations in order to minimize delay and budgetary strains caused by large numbers of investigations. Adoption of uniform basic investigative standards could eliminate this flexibility. Second, care must be exercised to ensure that the investigative programs of the more stringent agencies are not diluted with standards reflecting the lowest common denominator acceptable to all other agencies. Third, any basic standard must ensure that the resulting investigations will support both suitability and security determinations in order to avoid, as much as possible, duplicative expenditure of resources.

Further, the implementation of relatively uniform, basic investigative standards may require reassessment and realignment of investigative responsibilities and authorities in the future. For the present, however, it is thought best to avoid tampering with the current alignment and arrangements between and among OPM and the various departments and agencies and await the lessons of actual experience.

Agency Positions

The group agrees that an attempt should be made to develop reasonable uniform basic investigative standards that will preserve a fair degree of flexibility, avoid unreasonable resource burdens, and strengthen the weaker security programs while preserving those that are strong already.

RECOMMENDATION

That the NSDD-84 federal personnel security study group develop uniform basic investigative standards for access to national security information that reflect workable and appropriate distinctions between the various categories of such information.

________________________ Approved

________________________ Disapproved

ISSUE IV. - Adjudicative Standards Under A New Order

Should uniform basic procedural and due process standards be included for all access denials and revocations?

The practical effect on an individual of a clearance denial or revocation can differ significantly depending on the circumstances of that person's federal employment. For example, in some cases a denial or revocation can mean loss of employment or transfer to a less desirable position. Even where a denial does not have such drastic results, promotion potential could be affected. In these cases, the potential severity of a denial or revocation of access argues for a greater degree of procedural due process than might otherwise be established.

With a few exceptions, such as the Central Intelligence Agency, agencies must incorporate certain due process and appeal procedures into their adjudications for access to classified information in order to protect federal employees and to survive judicial scrutiny. Currently, except for fundamental requirements such as notice, each agency is more or less free to establish its own procedures.

As a result of Supreme Court decisions, there exists, pursuant to Executive Order 10865, an elaborate system of due process for industrial contractor personnel. Other systems of due process flow from the sensitivity of the information itself (See, for example, DCID 1/14 concerning SCI access).

The benefits of developing uniform procedures include simplicity and assurance that all persons will of necessity be treated in a similar manner regardless of their position or employing agency. Further, applying reasonable adjudication and appeal standards across the board increases significantly the extent to which government decisions in this area will be sustained in litigation and determined not to be arbitrary and capricious. Due process and procedural protections of some variety are required by the courts and need not remove or reduce the ultimate flexibility of the decisionmaker in determining whether access is in the best interests of the Government.

Agency Positions

The group agrees that uniform, basic due process standards for access adjudications should be developed that would preserve necessary agency flexibility but ensure fair and reasonable treatment for individuals.

RECOMMENDATION

That the NSDD-84 study group be authorized to develop basic uniform adjudicative procedures for denying or revoking access to classified information that are related to the impact an unfavorable determination may have on the person's status.

____________________ Approved

____________________ Disapproved

* * * * * * * *

With this guidance in hand, the group will proceed to develop more specific provisions and identify any more specific issues requiring your consideration.

/s/
MARY C. LAWTON
Counsel for Intelligence Policy
Office of Intelligence Policy and Review

EXHIBIT NO. 8

Office of the Attorney General
Washington, D.C. 20530

March 11, 1983

MEMORANDUM

TO: Heads of Offices, Boards, Divisions and Bureaus

FROM: William French Smith WFS
Attorney General

SUBJECT: Presidential Directive on Safeguarding National Security Information

The President has issued a directive to strengthen our efforts to safeguard national security information from unlawful disclosure. This directive, a copy of which is attached, is based upon the recommendations of an interdepartmental group chaired by the Department of Justice. I fully support the President's policy and expect that it will be faithfully implemented throughout the Department.

This directive does not alter the existing obligation of Department personnel to comply with statutes and regulations pertaining to national security information. We must be careful to avoid the unnecessary or improper use of classification. Whenever possible, information should be kept unclassified or declassified so as to permit public access. However, information that is properly classified in the interest of national security must be protected from unauthorized disclosure.

Many of the specific requirements of the directive involve no change from current Department of Justice policy.

-- The use of nondisclosure agreements and the requirement of prepublication review in appropriate cases are consistent with current policies. More detailed guidance on these policies will be provided in the near future.

-- The directive requires no change in existing Department policies on use of the polygraph, with regard to attorneys or FBI employees. Policies with regard to employees in the competitive service will be changed to conform with expected revisions in OPM regulations on this subject.

- Internal investigations of unauthorized disclosures will continue to be coordinated by the Office of Professional Responsibility, with assistance from the FBI as needed.

To the extent implementation of the President's directive requires changes in Department of Justice policies and procedures, you will be kept fully informed.

Safeguarding National Security Information

As stated in Executive Order 12356, only that information whose disclosure would harm the national security interests of the United States may be classified. Every effort should be made to declassify information that no longer requires protection in the interest of national security.

At the same time, however, safeguarding against unlawful disclosure of properly classified information is a matter of grave concern and high priority for this Administration. In addition to the requirements set forth in Executive Order 12356, and based on the recommendations contained in the interdepartmental report forwarded by the Attorney General, I direct the following:

1. Each agency of the Executive Branch that originates or handles classified information shall adopt internal procedures to safeguard against unlawful disclosures of classified information. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information. All such agreements must include a provision for prepublication review to assure deletion of SCI and other classified information.

c. All agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (ISOO), shall develop standardized forms that satisfy these requirements.

d. Appropriate policies shall be adopted to govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures of classified information. All persons with authorized access to classified information shall be clearly apprised of the agency's policies in this regard.

2. Each agency of the Executive branch that originates or handles classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

e. Persons determined by the agency to have knowingly made such disclosures or to have refused cooperation with investigations of such unauthorized disclosures will be denied further access to classified information and subjected to other administrative sanctions as appropriate.

3. Unauthorized disclosures of classified information shall be reported to the Department of Justice and the Information Security Oversight Office, as required by statute and Executive orders. The Department of Justice shall continue to review reported unauthorized disclosures of classified information to determine whether FBI investigation is warranted. Interested departments and agencies shall be consulted in developing criteria for evaluating such matters and in determining which cases should receive investigative priority. The FBI is authorized to investigate such matters as constitute potential violations of federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

4. Nothing in this directive is intended to modify or preclude interagency agreements between FBI and other criminal investigative agencies regarding their responsibility for conducting investigations within their own agencies or departments.

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate

adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations, and guidelines.

Embargoed for Conclusion of Background Briefing
Held March 11, 1983, at the Department of Justice

Fact Sheet

Presidential Directive on Safeguarding National Security Information

Background

-- Unlawful disclosures of classified information damage national security by providing valuable information to our adversaries, by hampering the ability of our intelligence agencies to function effectively, and by impairing the conduct of American foreign policy.

-- The President has issued a directive requiring that additional steps be taken to protect against unlawful disclosures of classified information.

-- This directive is based on the recommendations of an interdepartmental group convened by the Attorney General.

Scope of Directive

-- The directive deals only with disclosures of classified information.

-- By Executive Order, the only information that can be classified is information which "reasonably could be expected to cause damage to the national security" if released without proper authorization. (E.O. 12356 § 1.1(a)(3).)

-- The Executive Order also prohibits the use of classification to conceal violations of law, inefficiency or administrative error, or to prevent an embarrassment to a government agency or employee. (E.O. 12356 § 1.6(a).)

Summary of Provisions

-- The directive imposes additional restrictions upon government employees who are entrusted with access to classified information, and upon government agencies that originate or handle classified information.

> -- More employees will be required to sign nondisclosure agreements, including provisions for prepublication review, such as were approved by the Supreme Court in United States v. Snepp (1980).

  Agencies will be required to adopt policies concerning contacts between journalists and persons with access to classified information, so as to reduce opportunities for unlawful disclosures. However, no particular policies are mandated in the directive.

  - Agencies will be required to adopt new procedures so that unlawful disclosures of classified information will be reported and analyzed more efficiently.

- The directive establishes a new approach to investigating unlawful disclosures to replace the past practice of treating such matters as purely criminal investigations.

  - Although unauthorized disclosures of classified information potentially violate a number of criminal statutes, there has never been a successful prosecution. There are a number of practical barriers to successful criminal prosecution in most of these cases.

  - This directive clarifies FBI's authority to investigate unlawful disclosures of classified information, even though it is anticipated that a successful investigation will lead to administrative sanctions (such as demotion or dismissal) rather than criminal prosecution.

  - All agencies with employees having access to classified information will be required to assure that their policies permit use of polygraph examinations under carefully defined circumstances. The polygraph is already used on a regular basis by our largest intelligence agencies. The directive provides for a greater degree of consistency in government-wide policy regarding use of this investigative technique.

  - The use of the polygraph in any particular case will be subject to the discretion of an employee's agency head.

  - There will be no change in the current practice of targeting investigations at employees who are suspected of unlawfully disclosing classified information, rather than at journalists who publish it.

- The directive provides that employees found by their agency head to have knowingly disclosed classified information without authorization or to have refused cooperation with investigations will be subject to mandatory administrative sanctions to include, as a minimum, denial of further access to classified information. Existing procedural safeguards for personnel actions involving federal employees remain unchanged.

Expected Results

- This directive is not expected to eliminate all unlawful disclosures of classified information.

- The directive is designed to improve the effectiveness of our present program and, over time, to reduce the frequency and seriousness of unlawful disclosures of classified information.

- The directive also emphasizes that government employees who are entrusted with classified information have a fiduciary duty to safeguard that information from unauthorized disclosure.

The New York Times

Founded in 1851

ADOLPH S. OCHS, Publisher 1896-1935
ARTHUR HAYS SULZBERGER, Publisher 1935-1961
ORVIL E. DRYFOOS, Publisher 1961-1963

ARTHUR OCHS SULZBERGER, Publisher

A. M. ROSENTHAL, Executive Editor
SEYMOUR TOPPING, Managing Editor
ARTHUR GELB, Deputy Managing Editor
JAMES L. GREENFIELD, Assistant Managing Editor
LOUIS SILVERSTEIN, Assistant Managing Editor

MAX FRANKEL, Editorial Page Editor
JACK ROSENTHAL, Deputy Editorial Page Editor

CHARLOTTE CURTIS, Associate Editor
TOM WICKER, Associate Editor

JOHN D. POMFRET, Exec. V.P., General Manager
LANCE R. PRIMIS, Sr. V.P., Advertising
J. A. RIGGS JR., Sr. V.P., Operations
HOWARD BISHOW, V.P., Employee Relations
RUSSELL T. LEWIS, V.P., Circulation
JOHN M. O'BRIEN, V.P., Controller
ELISE J. ROSS, V.P., Systems

Extend the Ban on Censorship

Now that Congress's ban on the Administration's heavy-handed secrecy program is about to expire, the White House is making conciliatory noises to head off any extension. Congress ought not to take the bait.

President Reagan decreed a year ago that some extraordinary secrecy measures previously used only by the Central Intelligence Agency and the National Security Agency be extended to thousands of other Government employees. They were to be required to promise for the rest of their lives to submit any writings about national security to Government censors. They were also required to submit to random polygraph tests.

The order caused a storm of protest. Critics argued that the Administration had overreacted to only a few annoying but hardly threatening leaks of information. Congress quickly agreed that the order might actually damage the nation. It could hurt morale and also inhibit desirable criticism and analysis of foreign policy by former officials.

The Administration finally retreated last month and suspended its decree. Now Robert McFarlane, the President's national security adviser, offers voluntarily to extend the freeze through the current session of Congress and to take no further action without 90 days' advance notice.

But his letter displays an Administration unchastened by Congress's profound skepticism. "This is a serious problem that won't go away," he insists, "and we therefore cannot completely foreclose future action . . . if a legislative solution to unauthorized disclosures is not found."

The serious problem that "won't go away" is excessive Government secrecy. And for that the proper legislative solution is renewal of the law requiring the executive to desist unless it can make a stronger case for these ugly restraints.

8 THE NEW YORK TIMES, SATURDAY, MARCH 24, 1984

DELAY CONTINUED ON SECURITY RULE

White House Retreats Again From Its Censorship Plan

By **STUART TAYLOR Jr.**

Special to The New York Times

WASHINGTON, March 23 — The Reagan Administration has retreated another step from its plan to impose lifelong censorship and expanded polygraph, or lie-detector, testing of officials to guard national security secrets, according to correspondence made public this week.

Robert C. McFarlane, President Reagan's national security adviser, said in a March 20 letter that the censorship and polygraph provisions in a Presidential directive last year would not be reinstated "for the duration of this session of Congress." Congress is expected to adjourn in October.

His letter, to Representative Patricia Schroeder, Democrat of Colorado, followed an earlier Administration promise to suspend the provisions for an unspecified period. The letter was released by the Congresswoman's office.

Mr. McFarlane's letter said he wanted to "clarify the status of the directive" in order to dispel concerns in Congress that new legislation might be needed to block the Administration from reinstating the censorship and polygraph provisions.

A moratorium that Congress put on these provisions last year will expire April 15. Congress is considering whether to extend the ban. A bill to impose permanent restrictions on censorship and polygraph testing is pending before Representative Schroeder's Civil Service Subcommittee of the Post Office and Civil Service Committee.

Mr. McFarlane said the Administration might revive its censorship and polygraph program if it could not work out a solution with Congress to prevent "anonymous leaks to the press" and other unauthorized disclosures.

Mr. Reagan's directive of March 11, 1983, would require more than 100,000 officials who handle highly sensitive intelligence secrets to sign agreements consenting to "prepublication review" and official censorship of their writings for the rest of their lives. It would also require greatly expanded use of polygraph testing in investigations of unauthorized disclosures.

On Feb. 15, the Presidential spokesman, Larry Speakes, responding to sharp Congressional criticisms of the secrecy provisions, said Mr. Reagan "has agreed not to implement" them, pending efforts "to develop a bipartisan solution."

But until Mr. McFarlane's letter the Administration had provided no assurance that it would not reinstate the secrecy provisions as soon as the Congressional moratorium had expired.

Thursday, March 22, 1984 The Washington Post A21

McFarlane Acts on Reagan's Orders

New Polygraphs, Censorship Shelved

By George Lardner Jr.
Washington Post Staff Writer

The White House this week firmly pledged to abandon "for the duration of this session of Congress" its plans to expand the use of polygraph tests throughout the government and to impose a lifetime censorship system on officials having access to especially sensitive information.

The commitment was made in a March 20 letter to Rep. Patricia Schroeder (D-Colo.) from White House national security adviser Robert C. McFarlane, who said he was acting on President Reagan's instructions.

McFarlane also promised that the administration would give interested members at least 90 days' notice of any future action to deter leaks, "to facilitate congressional involvement" in such decisions.

The pledge appeared to signal the death of the most controversial aspects of a directive that Reagan issued in the name of national security a year ago. The House Post Office and Civil Service Committee, in turn, postponed a subcommittee session that had been scheduled yesterday to mark up a bill prohibiting the censorship and lie-detector programs. Congress voted last year to block them, but only through this April 15.

White House Counselor Edwin Meese III was a leading supporter of the Reagan effort to stop news "leaks," but White House chief of staff James A. Baker III and other presidential aides were strenuously opposed to the directive's most restrictive provisions.

Reagan's order would have required every federal employe with a security clearance to sign a non-disclosure pledge and to submit to lie detector tests if asked. It also said that those with so-called Sensitive Compartmented Information clearances would have to sign special agreements binding them, for life, to submit writings that might contain sensitive information, even if it was unclassified, for approval by government censors.

A General Accounting Office study said that the directive would have applied to 2.5 million federal employes and another 1.5 million employes of government contractors. The lifetime censorship rules would have applied to about 128,000 people.

Reagan said last month that he would suspend the directive's two key provisions. McFarlane followed with a memo telling affected government agencies that implementation should be "held in abeyance."

But House Government Operations Committee Chairman Jack Brooks (D-Tex.), the sponsor of a bill to block the effort permanently, said he feared that the suspension was just "a tactical postponement" to quiet the controversy before the fall elections.

In his letter, McFarlane said that leaks of classified information were "a serious problem that will not go away and we therefore cannot completely foreclose future action along the lines" of the directive "if a legislative solution to unauthorized disclosures is not found." But he repeated that no such action would be taken "for the duration of this session."

A13 THE NEW YORK TIMES, MONDAY, FEBRUARY 20, 1984

Secrecy Proposal: Risks Weighed Against Gains

By STUART TAYLOR Jr.

Special to The New York Times

News Analysis

WASHINGTON, Feb. 19 — Congress has forced President Reagan to back off, at least temporarily, from using more censorship and polygraph testing to protect national security, not because it thought the goal unimportant, but out of doubt that such measures would accomplish much.

In the view of Congressional critics, Mr. Reagan's plan would limit debate on vital issues and compromise the civil liberties of Government officials while doing little to prevent leakage of validly classified information and less to protect national security.

The opposition to two secrecy measures ordered by Mr. Reagan on March 11, 1983, forced the White House to announce last week that it would seek a "bipartisan solution" on the measures. The Administration apparently realized that Congress, which had already blocked these measures until April 15, was likely to extend the ban or make it permanent.

One measure would require more than 100,000 officials in the White House, the military and other departments who handle certain intelligence secrets to sign lifelong censorship agreements. The other would allow disciplinary sanctions against Government employees who refuse to take polygraph, or lie-detector, tests in investigations of unauthorized disclosures, or leaks.

What Degree of Protection

Few if any members of Congress have proposed prohibiting the censorship agreements and polygraph testing the executive branch has long required of intelligence agents. So the issue is not so much whether some freedoms must give way to protect national security as it is to what degree they must give way.

The Congressional position reflects a kind of cost-benefit analysis: The costs to civil liberties of the Reagan plan were seen as outweighing the benefits to the national security, benefits that some critics deemed negligible.

Richard K. Willard, the Justice Department official who was the principal architect of the measures, has stressed that the Congressional intelligence committees complained in the late 1970's that national security secrets were inadequately protected.

Thus, he asserted in an interview last week, if Congress will not support the Reagan secrecy plan, "it's time for Congress to come forward and say what their solution is to the problem." Meanwhile, Mr. Reagan has not revoked his March 11 order, only suspended it pending talks with Congress.

Security and Censorship

The Administration may have difficulty convincing Congress that the national security requires former officials to submit their writings and speeches for the rest of their lives for "prepublication review," or censorship, by their successors. Critics say such a requirement, at best, would inhibit debate and, at worst, could be used by incumbents as a pretext for silencing their critics.

William J. Casey, Director of Central Intelligence, said in a memorandum last year that such censorship agreements contain "the minimum acceptable standards for protecting the security" of intelligence sources and methods.

But Mr. Willard conceded that the censorship program would do nothing to prevent or detect espionage and little to prevent unauthorized disclosures.

"The most serious problem by far is the leak, the anonymous leak, and prepublication review does not prevent anonymous leaks," Mr. Willard acknowledged. "That's a much more difficult problem to address, but the disclosure of information in books and speeches was something we could do something about."

Few Disclosures Involved Secrets

The General Accounting Office found last year, in a survey of six agencies, that only 21 of the 328 unauthorized disclosures of classified information over a five-year period had occurred through former officials' writing or speeches. Only one or two of these involved intelligence secrets of the kind that would subject officials who handle them to lifelong censorship.

Such evidence led many Republicans as well as Democrats in Congress to conclude that the Reagan censorship program was a draconian solution to an almost nonexistent problem.

Mr. Willard has suggested that the censorship program would make its most important contribution by making Government employees and others sensitive to the need for secrecy, by putting some fear in them and thus by discouraging the rather casual trafficking in Government secrets long practiced by officials both high and low, reporters, lobbyists and others.

Such benefits, in the view of many in Congress, including Senator Charles McC. Mathias, Republican of Maryland, were too speculative to warrant a sweeping system of censorship.

The polygraph, say Mr. Willard and other Administration officials, is potentially very useful both for ferreting out those who leak Government secrets to the press and for catching foreign spies.

Fear of Machine Cited

They maintain not only that polygraph testing can detect lying in many cases but also that the fear of detection often spurs people to confess or deters them from leaking in the first place.

Congressional opponents of increased polygraph use, led by Representative Jack Brooks, Democrat of Texas, say they doubt this, and some experts assert that the polygraph is all but useless in detecting whether a person is lying.

Even those who concede that widespread polygraph use might uncover some leakers and spies question whether this would be worth the cost to the freedom and dignity of the innocent employees subject to the testing.

Some employees would falsely be branded as liars, just as some liars would incorrectly be identified as truthful, Mr. Brooks asserts. And even advocates of polygraph testing such as Mr. Willard concede that the machines and their operators sometimes make mistakes.

Another reason for the resistance to expanded polygraph testing is that many in Congress are of two minds about leaks, which have been denounced by every recent President, most forcefully by Mr. Reagan.

While there is strong sentiment for preventing Government employees from disclosing genuine military, intelligence and diplomatic secrets, many members recognize that the executive branch has long labeled as secret thousands of documents posing no threat whatsoever to national security and has sometimes done so to cover up politically embarrassing information.

The vast majority of disclosures of classified materials to the press and to Congress itself involve information that either has little to do with the national security or is already available to the Soviet Union and other nations. Members of Congress sometimes depend on such leaks in doing their jobs, and many would not want to see the employees responsible for them hunted down with polygraph machines.

A6 THE NEW YORK TIMES, FRIDAY, FEBRUARY 17, 1984

Democrats to Press Bills Against Secrecy Measures

By STUART TAYLOR Jr.
Special to The New York Times

WASHINGTON, Feb. 16 — Despite a White House effort to ease the dispute, Congressional Democrats said today that they would press their challenge to President Reagan's policy of using censorship and polygraph, or lie-detector, tests to guard national security secrets.

In addition, a spokesman for Senator Charles McC. Mathias Jr., Republican of Maryland, said Mr. Mathias wanted some further definitive action to "give a decent burial" to the censorship policy. The spokesman said the Senator planned to proceed with a hearing on the issue set for Feb. 21.

Democratic opponents of Mr. Reagan's secrecy measures welcomed a statement Wednesday by Larry Speakes, Mr. Reagan's chief spokesman, that the President had decided "not to implement" for the time being those aspects of an order on March 11, 1983, requiring vastly expanded use of censorship and polygraph testing of officials who handle certain intelligence secrets.

But the Democratic critics of the proposed secrecy measures stressed that Mr. Reagan had not committed himself to dropping the measures permanently. Some of the Democrats said they would go ahead with efforts to seek permanent legislation to block the Administration's continuing use of such measures and preventing Mr. Reagan from extending them.

Eagleton Questions Sincerity

"I question both the motives and the sincerity" behind Mr. Speakes's statement, said Senator Thomas F. Eagleton, a Missouri Democrat who cosponsored temporary legislation last year blocking the increased use of censorship agreements until April 15.

He said the President's motive was "to curtail a tidal wave of bad press until after the election" and to remove a controversial issue from the Senate hearings on the nomination of the White House counselor, Edwin Meese 3d, who helped draft Mr. Reagan's secrecy policies, to be Attorney General.

Mr. Mathias was the other sponsor of the temporary legislation blocking Mr. Reagan's efforts to require more than 100,000 officials who handle sensitive intelligence secrets to sign lifelong censorship agreements. He could not be reached today, his aides said.

A Tentative Move

Representative Jack Brooks, a Texas Democrat who is sponsoring a bill to impose tight, permanent restrictions on Government use of censorship and polygraphs, said Mr. Speakes's statement signaled "only a tentative half-step."

"Much of the Administration's polygraph and censorship scheme may still go forward," Mr. Brooks said. Under the approach announced by Mr. Speakes, he said, "each agency is free to enact their own version of the President's censorship and polygraph policies quietly in the shadows, agency by agency."

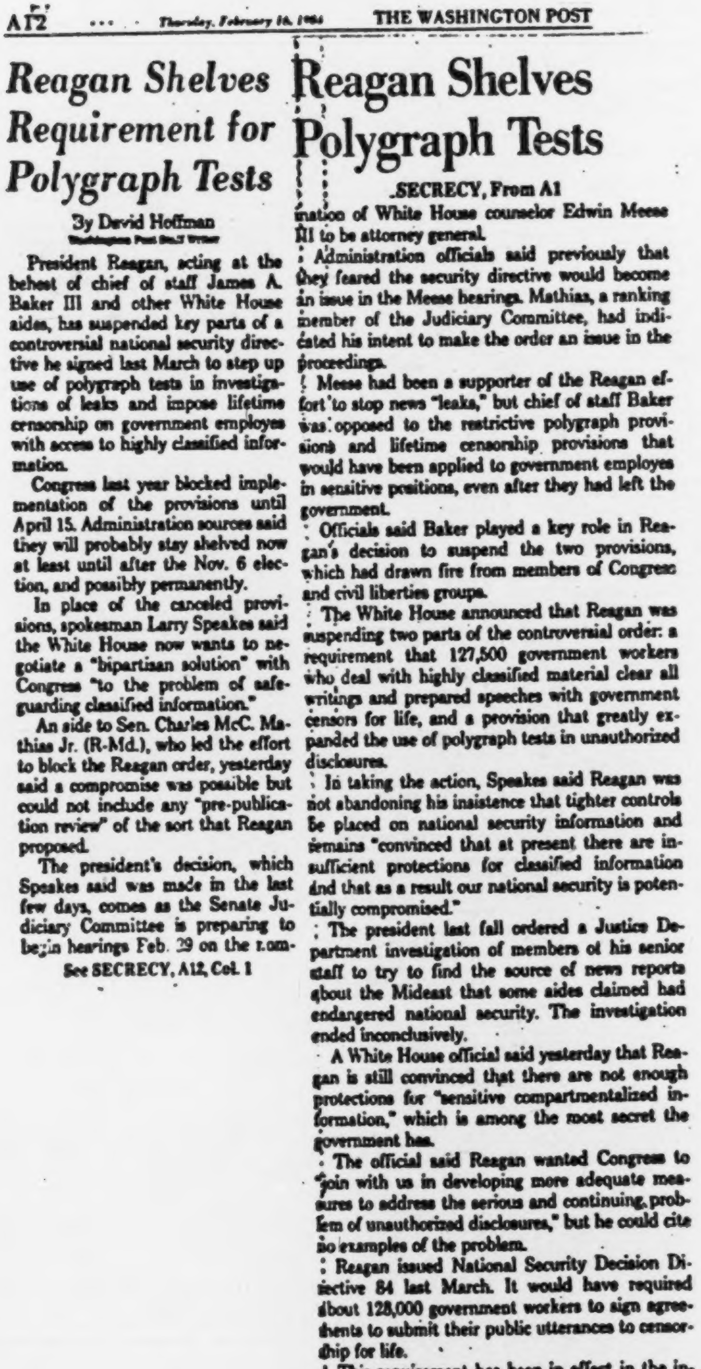
Brooks Pushes Legislation

Mr. Brooks noted that without new legislation the Defense Department apparently would be free after April 15 to proceed with its own plans to use polygraphs extensively "in employment interviews and for random security checks under the threat of adverse consequences," notwithstanding Mr. Speakes' statement. Mr. Brooks said enactment of his bill was necessary to prevent such measures.

Representative Patricia Schroeder, Democrat of Colorado, agreed, saying she planned to proceed with hearings on Mr. Brooks's bill before her subcommittee. She said that "random use of polygraphs and lifetime prepublication review restrictions have no place in a free society."

A White House official said today that Mr. Reagan had not yet signed any formal order suspending implementation of the censorship and polygraph provisions in the March 11, 1983, secrecy order, entitled "National Security Decision Directive 84."

The official added, "He intends to do so."



A12 Thursday, February 16, 1984 THE WASHINGTON POST

Reagan Shelves Requirement for Polygraph Tests

By David Hoffman
Washington Post Staff Writer

President Reagan, acting at the behest of chief of staff James A. Baker III and other White House aides, has suspended key parts of a controversial national security directive he signed last March to step up use of polygraph tests in investigations of leaks and impose lifetime censorship on government employes with access to highly classified information.

Congress last year blocked implementation of the provisions until April 15. Administration sources said they will probably stay shelved now at least until after the Nov. 6 election, and possibly permanently.

In place of the canceled provisions, spokesman Larry Speakes said the White House now wants to negotiate a "bipartisan solution" with Congress "to the problem of safeguarding classified information."

An aide to Sen. Charles McC. Mathias Jr. (R-Md.), who led the effort to block the Reagan order, yesterday said a compromise was possible but could not include any "pre-publication review" of the sort that Reagan proposed.

The president's decision, which Speakes said was made in the last few days, comes as the Senate Judiciary Committee is preparing to begin hearings Feb. 29 on the nom-

See SECRECY, A12, Col. 1

Reagan Shelves Polygraph Tests

SECRECY, From A1

ination of White House counselor Edwin Meese III to be attorney general.

Administration officials said previously that they feared the security directive would become an issue in the Meese hearings. Mathias, a ranking member of the Judiciary Committee, had indicated his intent to make the order an issue in the proceedings.

Meese had been a supporter of the Reagan effort to stop news "leaks," but chief of staff Baker was opposed to the restrictive polygraph provisions and lifetime censorship provisions that would have been applied to government employes in sensitive positions, even after they had left the government.

Officials said Baker played a key role in Reagan's decision to suspend the two provisions, which had drawn fire from members of Congress and civil liberties groups.

The White House announced that Reagan was suspending two parts of the controversial order: a requirement that 127,500 government workers who deal with highly classified material clear all writings and prepared speeches with government censors for life, and a provision that greatly expanded the use of polygraph tests in unauthorized disclosures.

In taking the action, Speakes said Reagan was not abandoning his insistence that tighter controls be placed on national security information and remains "convinced that at present there are insufficient protections for classified information and that as a result our national security is potentially compromised."

The president last fall ordered a Justice Department investigation of members of his senior staff to try to find the source of news reports about the Mideast that some aides claimed had endangered national security. The investigation ended inconclusively.

A White House official said yesterday that Reagan is still convinced that there are not enough protections for "sensitive compartmentalized information," which is among the most secret the government has.

The official said Reagan wanted Congress to "join with us in developing more adequate measures to address the serious and continuing problem of unauthorized disclosures," but he could cite no examples of the problem.

Reagan issued National Security Decision Directive 84 last March. It would have required about 128,000 government workers to sign agreements to submit their public utterances to censorship for life.

This requirement has been in effect in the intelligence community. Reagan would have expanded it.

The order disturbed some senior White House officials, none of whom signed it. The Republican-controlled Senate voted 56 to 34 last October to delay the plan for six months. Hearings are scheduled on the issue Feb. 23 in the Senate.

REAGAN TO RELENT ON SECRECY PLEDGE

Order on Polygraph Tests Also to Be Withheld, Aide Says

By LESLIE MAITLAND WERNER

Special to The New York Times

WASHINGTON, Feb. 14 — President Reagan has decided to suspend key provisions of a widely opposed national security order that would impose lifelong censorship on more than 120,000 Government officials and greatly expand the use of lie-detector tests, an Administration official said today.

The official said that these features of the directive, issued by Mr. Reagan last March but sidetracked on Capitol Hill, would be withheld while the Administration tried to negotiate a compromise with Congress.

"The President has decided to suspend those parts of the directive that are controversial, and where there has been a lack of understanding by Congress," the official said. "We are talking to Congress about ways that we could improve security without interfering with peoples' rights."

Use of Tests Increased

One provision that has aroused great opposition calls for an increase in the use of lie-detector, or polygraph, tests in inquiries into unauthorized disclosures of national security information. Another would require officials who handle highly classified information to sign pledges agreeing to submit, for the rest of their lives, any writings for

Continued on Page A20, Column 6

Reagan Reported to Relent on Secrecy Pledge

Continued From Page A1

"prepublication review" by Government censors.

Both these key provisions would be rescinded, the official said. Among other provisions, the order requires agencies to adopt new policies on reporting unauthorized disclosures of information and on contact between employees and journalists.

Several Administration officials said Mr. Reagan's decision was aimed at eliminating a potential political problem caused by widespread criticism of the far-reaching order.

One official said the White House was hoping "to remove it as a sore spot, a source of controversy" in an election year. Another suggested that if the White House did not reach a compromise with Congress, the President could reissue the order if re-elected.

Congress last year postponed implementation of Mr. Reagan's original directive until April 15, with some Republicans joining in attacking it. Senator Charles McC. Mathias Jr. of Maryland said it would create "a system which would allow the officials of one Administration to censor the writings of their predecessors."

White House Discussion

Internal debate about changing or withdrawing the controversial features of the order began more than a month ago, according to one Administration official involved. In a meeting in the Roosevelt Room of the White House a few weeks ago, he said, top members of the Administration discussed whether the rule should be withdrawn altogether or narrowed in scope.

The official said that among those present were Edwin Meese 3d, the White House Counselor; James A. Baker 3d, the chief of staff; Michael Deaver, the deputy chief of staff, and Fred Fielding, the White House counsel.

Also involved in the discussion, he said, was Richard K. Willard, the Justice Department official who has been chiefly responsible for drafting the Administration's program to guard national security secrets.

The official said that at the meeting, Mr. Willard opposed rescinding the order's key provision and argued instead for limiting the breadth of it by requiring prepublication review for a specified period, such as 10 or 15 years, rather than forever.

The official said that talk of rescinding the order during the meeting centered on the idea that unless the Administration did something itself to make the directive more palatable, it would be forced to deal with a solution provided by Congress.

The White House, this official and others said, seemed to be inclined to withdraw the controversial aspects of the order.

Mr. Willard, who is acting as chief of the Justice Department's civil division, said today the he could not comment on the officials' statements. Mr. Fielding did not return calls to his office.

As of two months ago, Reagan Administration officials acknowledged that not a single top Reagan official and only a handful of people in lower ranks had signed the new secrecy pledge. Aside from bureaucratic delays, they said they were attempting to proceed cautiously because of the opposition in Congress.

Opposed by A.C.L.U.

Around the same time, in a debate sponsored by the American Bar Association, Mr. Willard denied "that this Administration has done anything radically different from previous administrations" in attempting to safeguard national security.

But Floyd Abrams, a New York lawyer who has represented many news organizations in battles with the Government, described the Reagan policy as fundamentally different from that of previous administrations. A specialist in the First Amendment, Mr. Abrams contended that the Administration's "fixation" on national security came "at the expense of freedom of expression."

The American Civil Liberties Union has also spoken out against Mr. Reagan's directive. John Shattuck, its legislative director, said the order's policy on lie-detector tests raised constitutional questions. The directive warns Federal employees that an agency investigating an unauthorized disclosure of information might decide that "adverse consequences will follow an employee's refusal to cooperate with a polygraph examination."

Q.&A.: Richard K. Willard of the Justice Department

'Necessary Secrets' vs. the Public's Right to Know

Special to The New York Times

WASHINGTON, Oct. 24 — The Reagan Administration's campaign to stop unauthorized disclosures of national security secrets has come under attack from members of Congress, former officials, journalists and others who say that the means chosen do violence to the national traditions of free speech and open debate.

Much criticism has been focused on a national security decision directive issued by President Reagan March 11. One provision, which the Senate voted last week to block until April, requires more than 100,000 officials who handle especially sensitive intelligence secrets to sign agreements submitting to Government censorship for the rest of their lives. Another provision calls for vastly expanded use of polygraph tests to ferret out leakers and spies.

Richard K. Willard, a 35-year-old Deputy Assistant Attorney General, is the chief architect of these initiatives. Mr. Willard, a graduate of Harvard Law School who was a clerk for Associate Justice Harry A. Blackmun of the Supreme Court, discussed the issues in a recent interview. Here are excerpts.

•

Q. To some people this system of censorship and polygraph testing conjures visions of George Orwell's "1984." What's the justification?

A. The purpose of the Administration's program is to protect classified information from unauthorized disclosure. There are certain kinds of information that would cause serious damage to our country if that information became known publicly.

There's obviously a need to strike a balance between protecting necessary secrets and the public's right to know. In our view, though, over the last decade, the balance has swung too far in the direction of letting information become public, including some very sensitive information about intelligence activities. Our ability to conduct necessary intelligence activities has been severely compromised.

•

Q. Can you give one or two examples of harm that has been done through unauthorized leaks of classified information?

A. Examples of this are classified themselves. But, for example, if it comes out that we have a particular intelligence operation under way that was intended to remain secret, then it becomes much easier for our adversaries to take countermeasures.

•

Q. Does your censorship system sacrifice an important element of free speech out of concern for national security?

A. The agreement we've proposed would only require officials to submit things that they write about intelligence matters. Officials are free to write about anything else that they wish without prepublication review. In addition, the only officials who are covered are officials who have access to the most sensitive kinds of intelligence. We think the importance of protecting this very sensitive information outweighs the disadvantages that it may have for the employees.

The New York Times/Paul Hosefros

Richard K. Willard

Q. Would not the prepublication review system allow the officials of one administration to censor the writings of their predecessors?

A. There's a safeguard here — judicial review. If material is submitted for review and we try to take something out, we have to prove in court that every word we want to delete is classified, and properly classified.

•

Q. How do you answer critics who have suggested that each step further in this direction of censorship obscures the differences between the free society that we have and Soviet society, for example?

A. That sort of claim is absolutely ridiculous. Our proposal is a very moderate safeguard. Many free societies have much more severe restrictions. For example, Great Britain has the Official Secrets Act, which is much more rigorous than anything we have ever proposed. I think that critics who make that kind of accusation have absolutely no sense of proportion in viewing these issues.

The First Amendment is very important but there are other national interests as well, and the Supreme Court has recognized that First Amendment rights are not absolute. There is no First Amendment right for Government employees to disclose classified information without authorization.

•

Q. Is it a crime to publish or disclose classified information?

A. In most cases it is certainly a potential criminal violation.

•

Q. Experts say that using polygraph tests to screen large numbers of people may falsely brand innocent people as liars more often than such an approach catches guilty people. Would you dispute this, or, if not, how would you justify it?

A. Certainly the polygraph is not perfectly reliable. For that reason no action will be taken solely on the basis of polygraph examination results. Even so, there is some room for error that could be harmful to the employee. But for this very small number of highly sensitive positions, we think the national security interest outweighs the risk of harm to the individual employee and justifies the program. Our policy is to limit use of the polygraph to a very small number of very sensitive jobs. We oppose the use of the polygraph on a general basis in the Government.

I think we would all prefer to live in a world where we did not have to have intelligence agencies or be concerned about potential foreign adversaries, but that is not the case. Our goal is to protect as best we can that information without causing any unnecessary harm to the values of openness that we all share.

•

Q. Are you concerned about the possibility that some highly qualified people who object in principle to being censored or to polygraph testing might hesitate to join the Government?

A. These security requirements have been in place at the C.I.A. and other intelligence agencies for many years. We have proposed to extend some of these requirements to other people in the Government who have access to the same kind of sensitive classified information. We think that people who want to go to work for the Government in the area of national security and who have access to our country's most sensitive secrets must appreciate the need to take careful security precautions.

•

Q. Is there anything you'd like to add?

A. We have no desire to cut down on the flow of unclassified information to the press and public. We think that our policy represents a reasonable balance of the competing interests, but we do consider the protection of properly classified information to be a basic responsibility of the Government, and one that we intend to live up to.

Stuart Taylor Jr.

SENATORS PUT OFF STRICT CENSORSHIP URGED BY REAGAN

Move Would Bar Enforcement by Limiting Funds—House Passage Is Expected

By STUART TAYLOR Jr.

Special to The New York Times

WASHINGTON, Oct. 20 — The Senate voted today to block until at least April 15 President Reagan's new system of lifelong censorship for more than 100,000 officials handling highly sensitive information.

The 56-to-34 vote in the Republican-controlled chamber was considered a mild rebuff to the Administration and signaled rising concern in Congress about Mr. Reagan's directive of March 11 to protect national security secrets by expanded use of censorship and polygraph testing of officials.

The measure approved today, which supporters said would probably be adopted by the House as well, would apparently force the Administration to stop putting into effect its new requirement that officials of the Defense, State, Justice and other departments who handle highly classified "sensitive compartmented information" sign agreements consenting to "prepublication review" by Government censors of their writing for the rest of their lives.

Distribution Has Begun

The Administration has already begun distributing such agreements to be signed, and some of the more than 100,000 employees with access to "sensitive compartmented information" may have signed them already.

The effect of the language adopted by the Senate today was not entirely clear, because it would block the Administration only from carrying out a policy of requiring Federal employees to submit to censorship "after termination of employment with the Government."

Thus, the Administration would apparently remain free to censor people who handle sensitive information while they are with the Government. But it would apparently not be free to proceed with its plans to require employees to sign secrecy agreements consenting to submit to censorship even after they leave office.

The March 11 directive also called for vastly expanded use of polygraph, or lie-detector, examinations in investigations of unauthorized disclosures, or "leaks," of classified information to

Continued on Page A21, Column 3

THE NEW YORK TIMES, FRIDAY, OCTOBER 21, 1983

Senate Votes to Block Censorship

Continued From Page A1

members of the press and others.

While the amendment adopted today would not affect the Administration's use of polygraphs, another measure that limits the Defense Department's use of polygraphs was passed earlier this month.

President Reagan says he has the authority to carry out his secrecy order without approval by Congress, but he has not so far challenged the power of Congress to block the order by adopting new legislation.

The measure limits the authorization for various Government departments to use funds appropriated by Congress for the purpose of carrying out the censorship program.

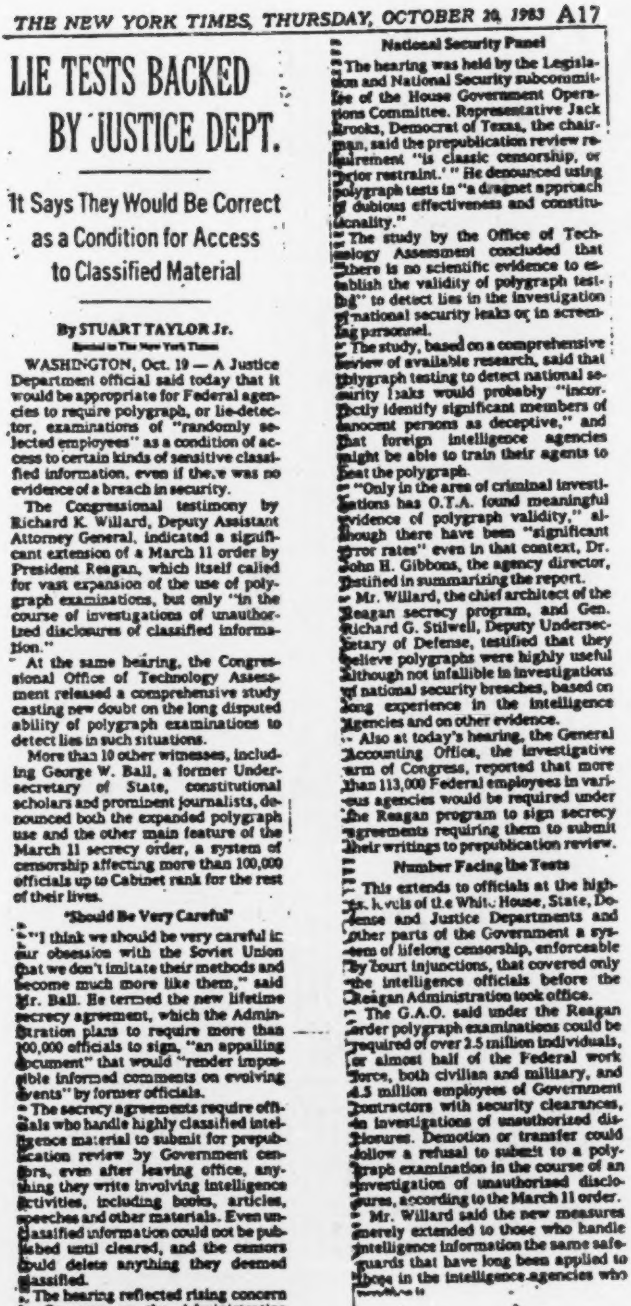
'Sweeping Prior Restraint'

Today's amendment, sponsored by Senators Charles McC. Mathias Jr., Republican of Maryland, and Thomas F. Eagleton, Democrat of Missouri, and supported by such key Republicans as Charles Percy, chairman of the Foreign Affairs Committee, was adopted as an amendment to the State Department's authorization bill for the fiscal years 1984 and 1985.

Mr. Reagan's directive, Mr. Mathias said in floor debate today, would create "a system which would allow the officials of one Administration to censor the writings of their predecessors," He said the prepublication review requirement amounted to "a sweeping program of prior restraint, a restriction on free speech which could pass muster under the First Amendment only if compelled by the most extraordinary circumstances."

Senator Mathias said the purpose of the amendment was to give Congress time to hold hearings on the Reagan directive, which the Administration put into effect without consulting Congress, and not necessarily to block it permanently.

Opponents of the amendment did not offer a detailed defense of the censorship program, but, rather, suggested that any problems could probably be worked out with the Administration without any legislation blocking it. Senator Jeremiah Denton, Republican of Alabama, stressed "harm to the United States" that had been caused by unauthorized disclosures of classified information.



THE NEW YORK TIMES, THURSDAY, OCTOBER 20, 1983 A17

LIE TESTS BACKED BY JUSTICE DEPT.

It Says They Would Be Correct as a Condition for Access to Classified Material

By STUART TAYLOR Jr.

Special to The New York Times

WASHINGTON, Oct. 19 — A Justice Department official said today that it would be appropriate for Federal agencies to require polygraph, or lie-detector, examinations of "randomly selected employees" as a condition of access to certain kinds of sensitive classified information, even if there was no evidence of a breach in security.

The Congressional testimony by Richard K. Willard, Deputy Assistant Attorney General, indicated a significant extension of a March 11 order by President Reagan, which itself called for vast expansion of the use of polygraph examinations, but only "in the course of investigations of unauthorized disclosures of classified information."

At the same hearing, the Congressional Office of Technology Assessment released a comprehensive study casting new doubt on the long disputed ability of polygraph examinations to detect lies in such situations.

More than 10 other witnesses, including George W. Ball, a former Undersecretary of State, constitutional scholars and prominent journalists, denounced both the expanded polygraph use and the other main feature of the March 11 secrecy order, a system of censorship affecting more than 100,000 officials up to Cabinet rank for the rest of their lives.

'Should Be Very Careful'

"I think we should be very careful in our obsession with the Soviet Union that we don't imitate their methods and become much more like them," said Mr. Ball. He termed the new lifetime secrecy agreement, which the Administration plans to require more than 100,000 officials to sign, "an appalling document" that would "render impossible informed comments on evolving events" by former officials.

The secrecy agreements require officials who handle highly classified intelligence material to submit for prepublication review by Government censors, even after leaving office, anything they write involving intelligence activities, including books, articles, speeches and other materials. Even unclassified information could not be published until cleared, and the censors could delete anything they deemed classified.

The hearing reflected rising concern in Congress as the Administration moves to implement its sweeping new measures to stop unauthorized disclosures of classified information to the press and others. Mr. Reagan says he has the authority to order such measures without Congressional approval but not many officials have not yet signed the new secrecy agreement.

National Security Panel

The hearing was held by the Legislation and National Security subcommittee of the House Government Operations Committee. Representative Jack Brooks, Democrat of Texas, the chairman, said the prepublication review requirement "is classic censorship, or 'prior restraint.'" He denounced using polygraph tests in "a dragnet approach of dubious effectiveness and constitutionality."

The study by the Office of Technology Assessment concluded that "there is no scientific evidence to establish the validity of polygraph testing" to detect lies in the investigation of national security leaks or in screening personnel.

The study, based on a comprehensive review of available research, said that polygraph testing to detect national security leaks would probably "incorrectly identify significant members of innocent persons as deceptive," and that foreign intelligence agencies might be able to train their agents to beat the polygraph.

"Only in the area of criminal investigations has O.T.A. found meaningful evidence of polygraph validity," although there have been "significant error rates" even in that context, Dr. John H. Gibbons, the agency director, testified in summarizing the report.

Mr. Willard, the chief architect of the Reagan secrecy program, and Gen. Richard G. Stilwell, Deputy Undersecretary of Defense, testified that they believe polygraphs were highly useful although not infallible in investigations of national security breaches, based on long experience in the intelligence agencies and on other evidence.

Also at today's hearing, the General Accounting Office, the investigative arm of Congress, reported that more than 113,000 Federal employees in various agencies would be required under the Reagan program to sign secrecy agreements requiring them to submit their writings to prepublication review.

Number Facing the Tests

This extends to officials at the highest levels of the White House, State, Defense and Justice Departments and other parts of the Government a system of lifelong censorship, enforceable by court injunctions, that covered only the intelligence officials before the Reagan Administration took office.

The G.A.O. said under the Reagan order polygraph examinations could be required of over 2.5 million individuals, or almost half of the Federal work force, both civilian and military, and 4.5 million employees of Government contractors with security clearances, in investigations of unauthorized disclosures. Demotion or transfer could follow a refusal to submit to a polygraph examination in the course of an investigation of unauthorized disclosures, according to the March 11 order.

Mr. Willard said the new measures merely extended to those who handle intelligence information the same safeguards that have long been applied to those in the intelligence agencies who [illegible]

U.S. Agencies Given Green Light for Random Lie Detector Tests

Agencies Get Green Light For Lie Tests

By George Lardner Jr.
Washington Post Staff Writer

The Reagan administration has given all government agencies the green light to require random lie detector tests for officials with access to especially sensitive information, even if they are not suspected of unauthorized disclosures.

The new policy was enunciated at a House subcommittee hearing yesterday by Deputy Assistant Attorney General Richard K. Willard, architect of the administration's controversial program of cracking down on leaks of classified information.

He said random tests would be useful in screening government employes cleared for so-called Special Access Programs, "to determine whether they have disclosed such information either to foreign agents or to others not authorized to receive it." Willard said it would be up to individual departments and agencies to decide whether they want to institute such a program, but he said it would be regarded as an "appropriate" counterintelligence device.

The Defense Department, according to another witness, already is prepared to "greatly expand" polygraph examinations at the Pentagon, including random tests of individuals with SCI (Sen-

See TEST, A14, Col. 2

TEST, From A1

sitive Compartmented Information) clearances.

House Government Operations Committee Chairman Jack Brooks (D-Tex.), who presided at the hearing, vowed to continue his campaign against polygraph testing. Under an amendment that Brooks helped tack onto the current Defense Department authorization bill, the Pentagon already has been ordered not to change its polygraph policy until April 15.

"I'm going after that amendment again next year," Brooks warned Richard G. Stilwell, deputy undersecretary of defense for policy. He added that Senate allies were trying to fashion another restrictive amendment that would be "broad enough to cover all government agencies." It may be offered as a rider on the State Department authorization bill.

Willard told a reporter during a break that he doubted that the State Department has plans to institute random polygraph tests, but indicated that some special units at the Justice Department may be inclined to do so.

Willard described his 49 pages of prepared testimony as "the first comprehensive enunciation of polygraph policy throughout the government," but Brooks kept Willard waiting for hours while others testified, urged him to give a quick summary when he was called, and said he would submit any questions for written response.

The controversy over President Reagan's campaign against leaks flared last March when he issued a directive, drafted by Willard, requiring every federal employe with a security clearance to sign a nondisclosure pledge and to submit to lie detector tests if asked.

The new order also required all those with SCI clearances to sign special agreements binding them, for life, to submit writings that might contain sensitive information, even if unclassified, to government censors.

Kenneth J. Coffey of the General Accounting Office testified that there are 112,660 SCI-cleared federal employes and another 15,090 contractor employes who would be subject to lifetime censorship, not counting those in the CIA and the National Security Agency where prepublication review agreements are standard practice.

A special GAO study showed that Reagan's March 11 directive would affect 2.5 million federal employes, about half of the 5.1 million civilian and military personnel, and another 1.5 million contractor employes.

The GAO study found 328 known unauthorized disclosures of classified information at agencies other than the CIA and the NSA, but apparently only two involved Sensitive Compartmented Information and those might have been deterred by the prepublication review agreements.

Former undersecretary of state George W. Ball told the subcommittee that the Reagan directive was "an appalling document" which "would require the establishment of a censorship bureaucracy far larger than anything known in our national experience."

"As a lawyer, I would fire a young attorney who drafted it," Ball declared as Willard sat in the audience. "I think it's an absurdity."

Other testimony dealt with conflicting opinions on the validity of the lie detector test. Dr. John H. Gibbons, director of the Congressional Office of Technology Assessment, said an exhaustive survey showed that "there is no scientific evidence to establish the validity of polygraph testing for screening a large number of people in connection with the investigation of unauthorized disclosures. There has been no research on this type of application."

"The instrument itself cannot detect deception," Gibbons said. "It's more of a fear detector than a lie detector." He said the OTA found "meaningful evidence of polygraph validity" only in criminal investigations, where a survey of acceptably scientific studies showed that "correct guilty detections ranged from 17 to 99 percent."

Willard contendedthat "the overwhelming majority of studies show accuracy rates . . . within the range of 70 to 95 percent."

He said the administration's polygraphy policy is "carefully limited" and provides that federal employes in competitive and uniformed services—as distinct from political appointees, those in the intelligence agencies and "other excepted services"—cannot be fired or demoted for refusing to take a polygraph exam. They can be denied access to classified information or reassigned, but Willard said such measures "are not considered to be adverse personnel actions."

The Presidential Directive and the Press

by Jay Peterzell

Several months after Leslie H. Gelb left his job as director of politico-military affairs at the State Department in 1981, he joined the Washington bureau of the *New York Times*. Since then, Gelb has brilliantly covered foreign policy, defense and arms control issues and has broken major stories about American diplomatic and covert intelligence operations abroad. Of course, it is controversial to hire former officials as journalists, and the editors of the *Times* thought long and hard before taking Gelb on. Apparently they made the right decision. But in the future, this sort of controversy could be purely academic because of a regulation about to be implemented by the Reagan administration.

The regulation, issued by President Reagan last March, requires officials with access to highly-classified information to agree to submit future writings to the government for pre-publication review. The measure generated considerable heat at the time among columnists, congressional committees and those in the administration concerned that government employees would henceforth be subject to censorship by their successors. The new directive, after all, applies to the thousands of officials in the White House, National Security Council, State Department, Pentagon and other agencies who have access to "sensitive compartmented information" (SCI), a category of classification above top secret.

Asked how these officials would be affected, administration spokesmen took refuge in a cloud of unknowing. They said an interagency committee was drafting an agreement officials would be required to sign. Until it was finished, they said, many questions above the directive simply could not be answered.

The committee has now completed its work. As of early August, the agreement faced one last round of review and approval, and was expected to be made public in a matter of weeks. The group has maintained strict secrecy about the details of the draft agreement, refusing to inform even congressional oversight committees about its deliberations. But other administration officials familiar with a July 1 "Final Draft" have described it privately as covering a very broad range of information.

According to these officials, the draft agreement requires a review of far more than the narrow category of SCI information. It also requires clearance for classified information from intelligence reports and formal "intelligence estimates," as well as all information concerning U.S. intelligence activities, whether classified or not. Moreover, once a manuscript has been submitted for review, government censors would be required to delete all other information they believe is classified even if it does not relate to intelligence matters.

The officials also said it had not yet been decided whether the review requirement would cover only information learned while in government service. If the final version of the agreement is not limited in this way, and if it covers a broad range of classified and unclassified information, in the future it will be virtually impossible for former officials to work as reporters.

Perhaps the simplest solution would be for news organizations not to hire former government employees. But the loss would be a significant one. The list of reporters who once held high security clearances, in addition to Gelb, includes William Beecher of *The Boston Globe*, Richard Inderfurth of *ABC News*, Hodding Carter of PBS' *Inside Story*, columnists Cord Meyer and William Safire, and quite a few others.

All of these journalists who could be reached for comment recently said their experience as officials had significantly helped them cover the government. They said this was not because they had learned classified information, but because they had become familiar with the substance of certain issues in great detail, or had learned how decisions are made, or had gotten to know people still in the bureaucracy. "It does make a difference whether you've spent your life looking in the keyhole or you've been in the room," commented Leslie Gelb. "You come to understand the workings of government in a different way."

The reporters also pointed out that a review government covering classified information learned after leaving the government would make it impossible for them to function. "In dealing with foreign policy and national security, you're frequently dealing with sensitive material," commented William Beecher. "No reporter would accept that kind of ground rule." Hodding Carter, the former State Department spokesman, put it this way: foreign affairs is an area in which "there is hardly anything you say to a reporter that isn't developed from classified material. Because they classify everything but the toilet paper." Carter also pointed out that officials by no means always tell reporters that information they have provided is classified.

Perhaps most disturbing, the Administration has not made any case for the new restrictions. The Defense Department recently sent Congress an analysis of sixty unauthorized disclosures of classified information. According to those who have seen the report, it identifies only one disclosure of SCI material. None of the disclosures occurred in new stories by former officials, and none would have been prevented by prepublication review.

A Senate subcommittee has now scheduled a hearing on the new directive for mid-September. The administration should give the Senate a chance to comment on the measure's effects on the press and other issues, rather than adopting a broad system of permanent censorship—in secret. ■

EXHIBIT NO. 9

U.S. MERIT SYSTEMS PROTECTION BOARD
Washington, D.C. 20419

February 20, 1985

Honorable Sam Nunn
Committee on Governmental Affairs
Senate Permanent Subcommittee
  on Investigations
United States Senate
Washington, D.C. 20510

Dear Senator Nunn:

In your letter dated January 29, 1985, you have requested a statement concerning the Board's views on the impact of the court's decision in *Hoska* v. *Department of the Army*, 677 F.2d 131 (D.C. Cir. 1982), on the Board's involvement in personnel security decisions. In *Hoska*, the court held that where an employee is removed based on revocation of a security clearance, the legality of the removal depends upon the legality of the revocation of the clearance. Thus, the agency's reasons for the revocation were held subject to review by the court.

Hoska was issued by the United States Court of Appeals for the District of Columbia prior to passage of the Federal Courts Improvement Act of 1982. Under that Act, the United States Court of Appeals for the Federal Circuit was created and was given exclusive jurisdiction to review non-mixed appeals decisions issued by the Merit Systems Protection Board. *See* 5 U.S.C. § 7703 (b)(1) (Supp. 1984). The Federal Circuit is not bound to follow the D.C. Circuit's decision in *Hoska* and the Federal Circuit has not yet decided the issue.

A large number of petitions for review of initial decisions issued in the regional offices involve the issue of security clearance revocations and the Board is currently reviewing its authority in this area. On December 13, 1984, and January 16, 1985, the Board published notices in the *Federal Register* which provided the opportunity for interested parties to file briefs on significant issues raised in those petitions for review. Copies of the Federal Register Notices are attached for your review. The Board has asked for briefs on the following issues:

(1) whether, in a case in which an employee's removal is based on revoking or denying the security clearance in appeals based substantially on an agency's revocation or denial of the employee's security clearance, the Board has the authority to review the agency's stated reasons for revoking or denying the security clearance;
(2) whether any law, rule or regulation concerning national security expressly or impliedly restricts the Board from such review;
(3) whether the Board has the authority to order an agency to reinstate a security clearance, and if not, whether there are alternative remedies available;
(4) whether an adverse action taken because of revocation of a security clearance may be taken under 5 U.S.C. § 7513 or whether section 7532 (suspension and removal actions taken in the interests of national security) is the exclusive basis for such an action.

Briefs on these issues must be filed no later than February 14, 1985. Final decisions will be issued by the Board after the briefs are considered. Since the issue of security clearance revocations is currently under review by the Board, it would be inappropriate at this time for the Board to comment further. Please note, however, that the issue of the Board's scope of review of security clearance revocations is an unsettled area of the law and Hoska may or may not be followed by the Board or the Federal Circuit.

When the Board's final decisions on security clearance revocations are issued, I will promptly forward copies to you. If I can be of any further assistance, please feel free to contact me.

Sincerely,

Paul E. Trayers
Legislative Counsel

local governments, and other interested parties became effective December 13, 1979, (44 FR 53685). Those practices and procedures are set out in revised § 250.34 of Title 30 of the CFR.

Dated: December 3, 1984.

John L. Rankin,

Regional Director, Gulf of Mexico OCS Region.

[FR Doc. 84-[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 4310-MR-M

INTERSTATE COMMERCE COMMISSION

[Ex Parte No. 388 (Sub-1)]

Intrastate Rail Rate Authority; Alabama

AGENCY: Interstate Commerce Commission.

ACTION: Notice of Decision.

SUMMARY: The Commission grants final certification to the Alabama Public Service Commission under 49 U.S.C. 11501(b) to regulate intrastate rail transportation.

DATE: Certification will begin on December 13, 1984.

FOR FURTHER INFORMATION CONTACT: Louis E. Gitomer, (202) 275–7245.

SUPPLEMENTARY INFORMATION: Additional information is contained in the Commission's decision. To purchase a copy of the full decision, write T.S. InfoSystems, Inc., Room 2227, Interstate Commerce Commission, Washington, DC 20423, or call 289-4375 (DC Metropolitan area) or toll free (800) 424-5403.

Decided: December 5, 1984.

By the Commission, Chairman Taylor, Vice Chairman Andre, Commissioners Sterrett, Gradison, Simmons, Lamboley, and Strenio.

James H. Bayne,

Secretary.

[FR Doc. 84-[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7035-01-M

[Ex Parte No. 388 (Sub-27)]

Intrastate Rail Rate Authority; Oregon

AGENCY: Interstate Commerce Commission.

ACTION: Notice of decision.

SUMMARY: The Commission has extended the provisional certification of Oregon under 49 U.S.C. 11501(b) to regulate Oregon intrastate rail transportation, pending submission of revised standards and procedures as noted in the full decision.

DATE: Oregon's provisional certification will expire February 11, 1985, unless prior to that date Oregon-files the required standards and procedures.

FOR FURTHER INFORMATION CONTACT: Louis E. Gitomer, (202) 275–7245.

SUPPLEMENTARY INFORMATION: Additional information is contained in the Commission's decision. To purchase a copy of the full decision, write to T.S. InfoSystems, Inc., Room 2227, Interstate Commerce Commission, Washington, DC 20423, or call 289-4357 (DC Metropolitan area) or toll free (800) 424-5403.

Decided: November 27, 1984.

By the Commission, Chairman Taylor, Vice Chairman Andre, Commissioners Sterrett, Gradison, Simmons, Lamboley, and Strenio. Chairman Taylor, joined by Commissioner Simmons, commented with a separate expression.

James H. Bayne,

Secretary.

[FR Doc. 84-[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7035-01-M

MERIT SYSTEMS PROTECTION BOARD

Federal Employees; Review of Agency Adverse Actions Taken Under 5 U.S.C. 7511 et seq. and Based Upon the Revocation or Denial of a Security Clearance

AGENCY: Merit Systems Protection Board.

ACTION: Notice of opportunity to file amicus briefs in certain appeals of agency adverse actions taken under 5 U.S.C. 7511 *et seq.* and based upon the revocation or denial of a security clearance.

SUMMARY: The Merit Systems Protection Board provides an opportunity to file amicus briefs on significant issues of law common to a number of cases pending before the Board involving appeals of agency adverse actions taken under 5 U.S.C. 7511 *et seq.* and based upon the agency's revocation or denial of the employee's security clearance.

DATE: Amicus briefs submitted in response to this notice shall be filed with the Acting Clerk of the Board on or before January 14, 1985.

ADDRESS: All briefs shall be captioned "Security Clearance Appeals," "Amicus Brief." All briefs shall also contain separate, numbered headings for each issue discussed. The original and twelve (12) copies of each amicus brief submitted in response to this notice shall be filed with the Office of the Clerk of the Board and addressed to Stephen E. Manrose, Acting Clerk, Merit Systems Protection Board, Attn: Security Clearance Appeals, 1120 Vermont Avenue, NW., Washington, D.C. 20419.

FOR FURTHER INFORMATION CONTACT: Stephen E. Manrose, Acting Clerk, Merit Systems Protection Board, (202) 653-7200. For copies of the Initial Decisions in the referenced cases, contact Research Services Division, Merit Systems Protection Board, (202) 653-7132.

SUPPLEMENTARY INFORMATION: The Systems Protection Board currently has before it numerous petitions for review of initial decisions issued by the Board's regional offices in security clearance appeals. The Board has identified several cases, listed below, which address significant issues of law common to a large number of these appeals and finds it appropriate to provide an opportunity for the filing of amicus briefs addressing these issues.

These cases include the following:

Bogdanowicz v. *Department of the Navy*, MSPB Docket No. PH07528110587 (January 18, 1984);

Egan v. *Department of the Navy*, MSPB Docket No. SE07528310257 (December 22, 1983);

Griffin v. *Defense Mapping Agency*, MSPB Docket No. SL07528410150 (July 6, 1984;

Peterson v. *Department of the Army*, MSPB Docket No. BN07528410010 (February 14, 1984).

Irving v. *Department of the Navy*, MSPB Docket No. BN07528410005 (September 21, 1984). (A petition for review is not pending in this appeal, in which a final order was issued by the Board. However, because this case concerns the issues identified in this notice, the Board is reopening this case to address these issues).

This notice represents the Board's offer to receive and consider amicus briefs from interested parties on the issues relevant to these appeals including:

I. Scope of the Board's Authority in Security Clearance Cases

A. Whether, in an adverse action case over which the Board has jurisdiction, and which is based substantially on the agency's revocation or denial of a security clearance, the Board has the authority to review the agency's stated reasons for revoking or denying the security clearance. Specifically address whether any law, rule or regulation concerning national security expressly or impliedly restricts the Board from from reviewing the agency's stated reasons for revoking or denying the security clearance.

B. Whether, if the Board has such authority, the Board's scope of authority extends to ordering the agency to reinstate the security clearance.

II. Alternative Remedies

A. If the Board's authority does not extend to ordering reinstatement of the security clearance, what alternative remedies may the Board order?

For the Board.

Dated: December 7, 1984.

Herbert E. Ellingwood,

Chairman.

[FR Doc. 84-32[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7400-01-M

NATIONAL SCIENCE FOUNDATION

Committee Management, Advisory Committee for Biological, Behavioral, and Social Sciences; Renewal

As required by the Federal Advisory Committee Act, Pub. L. 92-463, I have determined that the renewal of the Advisory Committee for Biological, Behavioral, and Social Sciences is necessary and in the public interest in connection with the performance of duties imposed upon the National Science Foundation by the National Science Foundation Act of 1950, as amended, and other applicable law. This determination follows consultation with the Committee Management Secretariat, General Services Administration.

Authority for the Advisory Committee for Biological, Behavioral, and Social Sciences shall expire on December 21, 1986, unless the Director of the National Science Foundation formally determines that continuance is in the public interest.

December 10, 1984.

Erich Bloch,

Director, National Science Foundation.

[FR Doc. 84-32[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7555-01-M

Advisory Panel for Ecology; Meeting

In accordance with the Federal Advisory Committee Act, as amended, Pub. L. 92-463, the National Science Foundation announces the following meeting:

Name: Advisory Panel for Ecology.

Date and time: January 10 and 11, 1985—8:30 a.m. to 5:00 p.m. each day.

Place: Room 1141, National Science Foundation, 1800 G St., NW., Washington, D.C. 20550.

Type of meeting: Closed.

Contact person: Dr. Patrick W. Flanagan, Program Director, Ecology (202) 357-9734, Room 1140, National Science Foundation, Washington, D.C. 20550.

Purpose of panel: To provide advice and recommendations concerning support for research in ecology.

Agenda: Review and evaluation of research proposals and projects as part of the selection process of awards.

Reason for closing: The proposals being reviewed include information of a proprietary or confidential nature, including technical information; financial data, such as salaries; and personal information concerning individuals associated with the proposals. These matters are within exemptions (4) and (6) of 5 U.S.C. 552b(c), Government in the Sunshine Act.

Authority to close meeting: This determination was made by the Committee Management Officer pursuant to provisions of section 10(d) of Pub. L. 92-463. The Committee Management Officer was delegated the authority to make such determinations by the Director, NSF, on July 6, 1979.

M. Rebecca Winkler,

Committee Management Officer.

December 10, 1984.

[FR Doc. 84-32[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7555-01-M

Advisory Panel for Geography and Regional Science; Meeting

In accordance with the Federal Advisory Committee Act, Pub. L. 92-463, as amended, the National Science Foundation announces the following meeting:

Name: Advisory Panel for Geography & Regional Science.

Date and time: January 14-16, 1984; 9:00 a.m. to 5:00 p.m.

Place: Room 540, National Science Foundation, 1800 G Street, NW, Washington, D.C.

Type of meeting: Closed.

Contact person: Dr. Ronald F. Abler, Program Director, Geography & Regional Science, Room 312, National Science Foundation, Washington, D.C. 20550; telephone (202) 357-7326.

Purpose of advisory panel: To provide advice and recommendations concerning support for research in Geography and Regional Science.

Agenda: Closed portion: To review and evaluate research proposals and projects as part of the selection process for awards.

Reason for closing: The proposals being reviewed include information of a proprietry or confidential nature, including technical information; financial data, such as salaries; and personal information concerning individuals associated with the proposals. These matters are within exemptions (4) and (6) of 5 U.S.C. 552b(c), Government in the Sunshine Act.

Authority to close meeting: This determination was made by the Committee Management Officer pursuant to provisions of section 10(d) of Pub. L. 92-463. The Committee Management Officer was delegated the authority to make such determinations by the Director, NSF, on July 6, 1979.

M. Rebecca Winkler,

Committee Management Officer.

[FR Doc. 84-32[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7555-01-M

Advisory Panel for Population Biology and Physiological Ecology; Meeting

In accordance with the Federal Advisory Committee Act, as amended, Pub. L. 92-463, the National Science Foundation announces the following meeting:

Name: Advisory Panel for Population Biology and Physiological Ecology.

Date and time: January 10 & 11, 1985—8:30 a.m. to 5:00 p.m. each day.

Place: Room 543, National Science Foundation, 1800 G St., NW., Washington, D.C. 20550.

Type of meeting: Closed.

Contact person: Dr. John L. Brooks, Acting Program Director, Population Biology and Physiological Ecology (202) 357-9728, Room 1140, National Science Foundation, Washington, D.C. 20550.

Purpose of panel: To provide advice and recommendations concerning support for research in population biology and physiological ecology.

Agenda: Review and evaluation of research proposals and projects as part of the selection process of awards.

Reason for closing: The proposals being reviewed include information of a proprietary or confidential nature, including technical information; financial data, such as salaries; and personal information concerning individuals associated with the proposals. These matters are within exemptions (4) and (6) of 5 U.S.C. 552b(c), Government in the Sunshine Act.

Authority to close meeting: This determination was made by the Committee Management Officer pursuant to provisions of section 10(d) of Pub. L. 92-463. The Committee Management Officer was delegated the authority to make such determinations by the Director, NSF, on July 6, 1979.

M. Rebecca Winkler,

Committee Management Officer.

December 10, 1984.

[FR Doc. 84-32[illegible] Filed 12-12-84; 8:45 am]

BILLING CODE 7555-01-M

Advisory Panel for Systematic Biology; Meeting

In accordance with the Federal Advisory Committee Act, as amended, Pub. L. 92-463, the National Science Foundation announces the following meeting:

Name: Advisory Panel for Systematic Biology.

Date and time: January 14 & 15, 1985—8:30 a.m. to 5:00 p.m. each day.

determination from the presiding officer in the above-captioned investigation terminating the following respondents on the basis of a consent order agreement: TUI Industrial Co., Ltd., Mao Shan Machinery Industrial Co., Ltd. and Union Tool Exporters, Ltd.

SUPPLEMENTARY INFORMATION: This investigation is being conducted pursuant to section 337 of the Tariff Act of 1930 (19 U.S.C. 1337). Under the Commission's rules, the presiding officer's initial determination will become the determination of the Commission thirty (30) days after the date of its service upon the parties, unless the Commission orders review of the initial determination. The initial determination in this matter was served upon the parties on January 10, 1985.

Copies of the initial determination, the consent order agreement, and all other nonconfidential documents filed in connection with this investigation are available for inspection during official business hours (8:45 a.m. to 5:15 p.m.) in the Office of the Secretary, U.S. International Trade Commission, 701 E Street NW., Washington, D.C. 20436, telephone 202-523-0161.

Written Comments

Interested persons may file written comments with the Commission concerning termination of the aforementioned respondents. The original and 14 copies of all such comments must be filed with the Secretary to the Commission, 701 E Street, NW., Washington, D.C. 20436, no later than 10 days after publication of this notice in the Federal Register. Any person desiring to submit a document (or portion thereof) to the Commission in confidence must request confidential treatment. Such requests should be directed to the Secretary to the Commission and must include a full statement of the reasons why confidential treatment should be granted. The Commission will either accept the submission in confidence or return it.

FOR FURTHER INFORMATION CONTACT: Ruby J. Dionne, Office of the Secretary, U.S. International Trade Commission, Telephone 202-523-0176.

By order of the Commission.

Issued: January 8, 1985.

Kenneth R. Mason,

Secretary.

[FR Doc. 85-1269 Filed 1-15-85; 8:45 am]

BILLING CODE 7020-02-M

MERIT SYSTEMS PROTECTION BOARD

Federal Employees; Review of Agency Adverse Actions Taken Under 5 U.S.C. 7511 et seq. and Based Upon the Revocation or Denial of a Security Clearance

AGENCY: Merit Systems Protection Board.

ACTION: Amendment to 49 FR 48623 (1984), affording notice of opportunity to file amicus briefs in certain appeals of agency adverse actions taken under 5 U.S.C. 7511 *et seq.* and based upon the revocation or denial of a security clearance.

SUMMARY: The Merit Systems Protection Board provides an opportunity to file amicus briefs on significant issues of law common to a number of cases pending before the Board involving appeals of agency adverse actions taken under 5 U.S.C. 7511 *et seq.* and based upon the agency's revocation or denial of the employee's security clearance.

This amendment supplements a previous notice (49 FR 48623 (1984)), to identify one additional issue for briefing by interested parties, identify four additional cases, and to extend the time for briefing on all issues.

DATE: Amicus briefs submitted in response to this notice, as well as the previous notice published at 49 FR 48623 (1984), shall be filed with the Clerk of the Board on or before February 14, 1985.

ADDRESS: All briefs shall be captioned "Security Clearance Appeals." "Amicus Brief." All briefs shall also contain separate, numbered headings for each issue discussed. The original and twelve (12) copies of each amicus brief submitted in response to this notice shall be filed with the Office of the Clerk of the Board and addressed to Robert E. Taylor, Clerk, Merit Systems Protection Board, Attn: Security Clearance Appeals, 1120 Vermont Avenue, NW., Washington, D.C. 20419.

FOR FURTHER INFORMATION CONTACT: Robert E. Taylor, Clerk, Merit Systems Protection Board, (202) 653-7200. For copies of the Initial Decisions in the referenced cases, contact Research Services Division, Merit Systems Protection Board, (202) 653-7132.

SUPPLEMENTARY INFORMATION: The Merit Systems Protection Board currently has before it numerous petitions for review of initial decisions issued by the Board's regional offices in security clearance appeals. The Board identified several cases, listed below, which address significant issues of law common to a large number of these appeals and in previous notice (40 FR 48623 (1984)), provided an opportunity for the filing of amicus briefs addressing these issues. The cases identified in that earlier notice were the following:

Bogdanowicz v. *Department of the Army,* MSPB Docket No. PH07528110587 (January 18, 1984);
Egan v. *Department [illegible] Navy,* MSPB Docket No. SE075[illegible]57 (December 22, 1983);
Griffin v. *Defense Mapping Agency,* MSPB Docket No. SL07528410150 (July 6, 1984);
Petersen v. *Department of the Navy,* MSPB Docket No. BN07528410010 (February 14, 1984);
Irving v. *Department of the Navy,* MSPB Docket No. BN07528410005 (September 21, 1984). (A petition for review is not pending in this appeal, in which a final order was issued by the Board. However, because this case concerns the issues identified in this and the previous notice, the Board is reopening this case to address those issues).

The Board now adds the following cases to those listed in the earlier notice:

Skees v. *Department of the Navy,* MSPB Docket No. PH07528410257 (June 14, 1984);
Holtcamp v. *Department of the Navy,* MSPB Docket No. SE07528410105 (June 21, 1984);
Drake v. *Department of the Army,* MSPB Docket No. AT07528310651 (November 9, 1983);
Gibson v. *Defense Mapping Agency,* MSPB Docket No. AT07528410438 (June 28, 1984);

In addition to the issues listed in the previous notice, the Board also requests interested parties to address the following question:

I. Scope of the Board's Authority in Security Clearance Cases

C. When an agency wishes to base an action listed in 5 U.S.C. 7512 on the revocation of security clearance, may it do so pursuant to 5 U.S.C. 7513, or is 5 U.S.C. 7532 the exclusive basis for such an action?

The time limit set by the Board in its earlier notice is now extended to February 14, 1985, for filing briefs as to issues identified in both the earlier notice and in this notice.

Dated: January 11, 1985.

For the Board.

Herbert E. Ellingwood,

Chairman.

[FR Doc. 85-1159 Filed 1-15-85; 8:45 am]

BILLING CODE 7400-01-M

EXHIBIT NO. 10

CLEARED SOVIET ÉMIGRÉS

	NUMBER
TOP SECRET	121
SECRET	1,349
CONFIDENTIAL	23
TOTAL	1,493

MAJOR FACILITIES EMPLOYING SOVIET ÉMIGRÉS

	NUMBER
HUGHES	95
LOCKHEED	68
TRW	39
GRUMMAN	36

ÉMIGRÉS FROM FOREIGN COUNTRIES
CLEARED/ INPROCESS

ALBANIA — 17
BULGARIA — 55
CAMBODIA — 24
PR CHINA — 3,291
CUBA — 1,056
CZECHOSLOVAKIA — 574
NORTH KOREA — 51
EAST GERMANY — 257
HUNGARY — 947
LAOS — 14
POLAND — 1,225
ROMANIA — 354
USSR — 1,555
VIETNAM — 670
YUGOSLAVIA — 585

TOTAL — 10,675

DISCO: NUMBER OF CONTRACTORS SUBMITTING 6.b.1 REPORTS

REGION	FY 84 TOTAL	% OF FACILITIES vs NO. OF REPORTS	FY 85 TO DATE	% OF FACILITIES vs NO. OF REPORTS
NEW ENGLAND	66	4%	42	2%
MID-ATLANTIC	47	2%	55	3%
CAPITAL	117	5%	91	3%
MID-WESTERN	38	3%	37	3%
SOUTHEASTERN	70	5%	69	5%
SOUTHWESTERN	77	7%	64	5%
NORTHWESTERN	44	4%	52	5%
PACIFIC	120	5%	89	4%
TOTALS	579	4%	499	4%

EXHIBIT NO. 11

NINETY-NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT OPERATIONS

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515

MAJORITY MEMBERS
JACK BROOKS, TEXAS, CHAIRMAN
DON FUQUA, FLORIDA
JOHN CONYERS, JR., MICHIGAN
CARDISS COLLINS, ILLINOIS
GLENN ENGLISH, OKLAHOMA
HENRY A. WAXMAN, CALIFORNIA
TED WEISS, NEW YORK
MIKE SYNAR, OKLAHOMA
STEPHEN L. NEAL, NORTH CAROLINA
DOUG BARNARD, JR., GEORGIA
BARNEY FRANK, MASSACHUSETTS
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
BARBARA BOXER, CALIFORNIA
SANDER M. LEVIN, MICHIGAN
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
JOHN M. SPRATT, JR., SOUTH CAROLINA
JOE KOLTER, PENNSYLVANIA
BEN ERDREICH, ALABAMA
GERALD D. KLECZKA, WISCONSIN
ALBERT G. BUSTAMANTE, TEXAS
MATTHEW G. MARTINEZ, CALIFORNIA

MINORITY MEMBERS
FRANK HORTON, NEW YORK
THOMAS N. KINDNESS, OHIO
ROBERT S. WALKER, PENNSYLVANIA
WILLIAM F. CLINGER, JR., PENNSYLVANIA
ALFRED A. (AL) McCANDLESS, CALIFORNIA
LARRY E. CRAIG, IDAHO
HOWARD C. NIELSON, UTAH
JIM SAXTON, NEW JERSEY
PATRICK L. SWINDALL, GEORGIA
THOMAS D. (TOM) DELAY, TEXAS
DAVID S. MONSON, UTAH
JOSEPH J. DioGUARDI, NEW YORK
JOHN G. ROWLAND, CONNECTICUT
RICHARD K. ARMEY, TEXAS
JIM LIGHTFOOT, IOWA
JOHN R. MILLER, WASHINGTON

MAJORITY—225-5051
MINORITY—225-5074

April 29, 1985

The Honorable Sam Nunn
SD-303
U.S. Senate
Washington, D.C. 20510

Dear Senator Sam

Please find enclosed written testimony for the Governmental Affairs Permanent Subcommittee on Investigations hearings of April 16-18 on personnel security matters. I request that you submit it for the record at those hearings and I urge you to take a hard look at this entire polygraph fiasco.

With every good wish, I am

Your friend

Sincerely,

Jack Brooks

Jack Brooks
Chairman

Statement of Congressman Jack Brooks
Permanent Subcommittee on Investigations
Senate Committee on Governmental Affairs
April 16-18, 1985

My views on polygraphs are by now well known. I have been engaged in the debate over their use and abuse for many years as a Member, and now Chairman, of the House Government Operations Committee. This Committee has overseen the government's polygraph programs since the early 1960's. I need not review the history here. Suffice it to say the Federal government's use of polygraphs has shown tremendous growth in the last several years.* In fact, this Administration has offered it as a centerpiece of its efforts to enhance our government's personnel and information security programs.

The President's National Decision Security Directive 84 would have mandated coerced use of the polygraph on Federal employees in all executive agencies in the course of media "leak" investigations. Various agencies, foremost of which is the Defense Department, have sought authority to begin massive coerced polygraph screening programs--pre-employment and random checks--for personnel security purposes. The Government Operations Committee has strongly recommended against those measures in its report "The Administration's Initiatives to Expand Polygraph Use and Impose Lifelong Censorship on Thousands of Government Employees," House Report 98-578. In two other separate reports over the last twenty years the Government Operations Commmittee has made similar recommendations (House Reports 80-198 and No. 94-795).

I believe that any informed review of polygraph use must keep two important points in mind. First, there is a difference between uncoerced polygraph use in carefully controlled investigations into specific incidents of misbehavior and their use to "screen" persons without strong suspicion of specific wrongdoing.

---

*Attached is an article prepared by me which treats the history of Federal Polygraphs policies, "Polygraph Testing--Thoughts of a Skeptical Legislator," American Psychologist, Vol 40, No. 3, March 1985.

This is true in terms of both the scientific evidence for the polygraph's validity and for concerns about unwarranted intrusion and individual privacy. The Office of Technology surveyed the scientific literature on polygraph validity for the Government Operations Committee's recent review. In its report--Scientific validity of polygraph testing: A research review and evaluation (OTA-TM-H-15, November 1983)--the OTA concluded that there was no scientifically acceptable study to support the use of polygraphs for screening purposes and that any validity that the polygraph test may have for specific incident use would likely decrease dramatically in that screening context. With regard to privacy it is, of course, a fundamental tenet of American justice, that searches or interrogations must be premised upon a well-grounded suspension of misbehavior. Polygraph screening is a direct affront to this American precept.

Second, the fundamental importance of the scientific validity of polygraph testing to evaluating the merits of polygraphing is clear. If polygraph testing does not work for the purpose intended--to catch lies--it should not be used whatever the privacy concerns suggest. OTA's findings on validty raise doubts about the specific-incident investigatory use of polygraphs as well as for screening. In 28 studies presenting "acceptable scientific criteria" in the specific-incident context, correct guilty detections ranged from 35% to 100%. Correct innocent detections ranged from 12.5% to 94%. None of those studied national security investigations. Further, OTA found that, in any context, coercing persons to take a polygraph test would likely affect validity negatively. No research has been done on that point.

Since OTA's study, the proponents of polygraph use have backed away from their claims of high polygraph validity. Instead, they argue the concept of utility. They point to numerous instances when the polygrap exam, or the threat of the exam, has been useful in eliciting important information or even confessions. Refined, this is the Nixon maxim of the Watergate tapes--"I don't know how accurate they are, but I do know that they'll scare the hell out of people."

This utility, however, ultimately rests on one's belief in the machine's validity. Indeed, the examiner spends a tremendous portion of the exam attempting to convince the person being examined that the machine will catch them lying. That utility will evaporate quickly, if it hasn't already, precisely in the instances when the government needs it most--the detection of highly trained and sophisticated moles and spies. A policy premised on a myth cannot remain effective long, especially when it is spread far and wide.

I strongly believe that security concerns alone argue against the use of polygraph screening by the Federal government. And I have introduced legislation to that effect.

My bill, H.R. 39--The Federal Polygraph Limitation and Anti-Censorship Act of 1985--(attached) would prohibit the use of polygraph testing for screening purposes and tightly control their use in criminal investigations. They could be used for that purpose only on a truly voluntary basis. These prohibitions would apply to all Federal agencies except for the CIA and the NSA.

After many years of bureaucratic initiatives in this area, I feel it is time for Congress to set a rational polygraph policy. It is much too serious of a matter to be left with the polygraph practitioners. As was pointed out in a recent article in The Atlantic Monthly (attached) polygraphing now constitutes a "flourishing" industry and reliance on the views of the practitioners is like accessing the "science" of astrology by sending a questionnaire to astrologers.

Reprinted from AMERICAN PSYCHOLOGIST. Vol. 40, No. 3, March 1985
Printed in U. S. A.

Polygraph Testing

Thoughts of A Skeptical Legislator

Jack Brooks *U.S. House of Representatives*

ABSTRACT: The controversy over the use of polygraphs by the federal government is not new. There has been a long history of debate within the government over the propriety and wisdom of using the "lie detector." Nonetheless, the federal government, under the leadership of the Reagan administration, is expanding the use of such tests for screening and investigative purposes. This article reviews the history of debate within the government over the use of the polygraph, and it describes legislation that must be enacted to control the proliferation of unwarranted and inaccurate polygraph use.

It has been with an eerie sense of *deja vu* that I have watched events regarding this Administration's proposal for polygraph use unfold. As a young representative in the early 1960s, I witnessed a similar scenario played out in Washington. There was a major difference though with how President Kennedy reacted to the use of polygraph tests. When details of the widespread threat of polygraph testing during the course of a "leak" investigation at the Defense Department came to light, President Kennedy publicly intervened and stopped the investigation before any tests were administered. At a news conference he indicated that it was "a mistake to suggest a polygraph," and added, "I don't think we need concern ourselves in the future about it" (*Public Papers of the Presidents,* 1963, p. 304).

Unfortunately, President Kennedy's assurances that polygraph tests would not be used no longer prevail in Washington. Recently, the Defense Department (DOD) conducted a "leak" investigation that involved the polygraphing of over 30 Defense Department employees. Further, DOD has proposed revisions to their regulations regarding polygraphs that would greatly increase the use of, and reliance on, polygraphs during investigations and in noninvestigatory contexts as well.

President Reagan, professing to be "up to his kiester in leaks" has endorsed the polygraph as his solution and issued a presidential directive (U.S. Department of Justice, 1983) requiring each agency to issue regulations that, at a minimum, provide that "employees may be required to submit to polygraph examinations," under the threat of "adverse consequences" (p. 3) if they refuse. Other employees would be subject to preemployment and random screening. This directive and the proposed Defense Department regulations changes would overturn existing rules governing polygraph use throughout the nonintelligence agencies of the federal government. These rules were established in response to congressional and Administration recommendations made back in the early 1960s following the DOD investigation and subsequent congressional review.

In response to this major policy reversal, several committees of Congress held hearings, and legislation was introduced in the House to control government use of polygraph tests. The Government Operations Committee, which I chair, takes a major role overseeing polygraph tests in the federal government. As part of its oversight activities, the committee asked the Office of Technology Assessment (OTA) for information that would assist it in deciding on the wisdom of expanding polygraph use. OTA was established in 1972 to provide nonpartisan information and advice to Congress on scientific and technological issues. The committee also requested studies by the General Accounting Office (GAO) on the scope of polygraph use by the federal government.

From 1963 to 1976, congressional investigations into polygraph use had consistently found that the scientific research base on the validity of polygraph testing was both conflicting and woefully inadequate. More and better research had been a recommendation of most committee reports. When the issue resurfaced in 1983, we thought that the scientific community might have shed new light on the validity of polygraph testing. We needed to know the state of current knowledge on polygraph testing. What was the theory behind it? What was the evidence to support its use? What implications did polygraph testing research have for the proposed changes in government policy?

What follows is a brief history of congressional interest in polygraph testing and events leading to legislative proposals to limit use of polygraph tests with government employees. As this article goes to press, the federal government is still trying to develop

Copyright 1985 by the American Psychological Association, Inc. 0003-066X/85/$00.75
Vol. 40, No. 3, 348–354

a consensus about polygraph use. By virtue of our investigation and OTA's report, the scientific picture has become more complicated. However, the need to control expansion of this technology seems ever more clear.

The History

A memo "leaked" from the Air Force about development of the TFX fighter plane captivated the attention of Washington for a short period during the spring of 1963 and invoked the ire of President Kennedy. The circumstances surrounding the probe into the leak are strikingly similar to those that induced the Reagan administration 20 years later to focus on the polygraph as the centerpiece of its information and personnel security program. The TFX controversy publicly surfaced in March 1963 when the Washington *Evening Star* had a lead article (Fryklund, 1963) that featured an internal Air Force memorandum. The memorandum charged investigators for a Senate committee that was looking into a $6.5 billion award to General Dynamics for the TFX (later redesignated the F-111 to avoid the bad publicity), with "oral abuse and pressure tactics" (p. 1). Robert McNamara, then Secretary of Defense, ordered the Secretary of the Air Force to find the source of the leak. Although the memorandum was unclassified, it was felt to be very damaging to the department. Air Force Secretary Zuckert called upon his Inspector General to conduct the investigation, giving him a free hand.

The free hand meant that all of the 120 department employees interviewed in the investigation, including the Secretary of the Air Force and other presidential appointees, were asked to sign a written agreement indicating their willingness to take a polygraph examination. Serious problems developed, however, when an Assistant Secretary of Defense refused as a matter of principle to sign the agreement. Media reports of the refusal and Pentagon officials' descriptions of the threatened use of polygraphs as standard, although concealed, investigatory practice at the department, led to President Kennedy's rebuke. It later led to an abandonment of the investigation and a study of DOD's polygraph policies ordered by the Secretary of Defense. The *New York Times* ("Lie Detectors in the Pentagon," 1963) highlighted the incident with an editorial characterizing this threatened use of polygraphs as "investigative methods that have reached a new low in the Defense Department and have harmed service morale" (p. 18).

Jack Brooks

It was against this backdrop that Representative Dawson, Chair of the Government Operations Committee of the House of Representatives, asked the Foreign Operations and Government Information Subcommittee to study the federal government's use of polygraphs. The Government Operations Committee (which I have chaired since 1975) is the chief

---

Editors note. Representative Jack Brooks (D-Texas) has been a member of the U.S. Congress since 1952. Prior to his election to the House, Representative Brooks was a member of the Texas House of Representatives from 1946 to 1950. Representative Brooks has held many leadership positions in Congress. From 1955 to 1974, he served as chair of the House Subcommittee on Government Activities, and from 1975 to the present he has chaired the House Government Operations Committee, as well as the Subcommittee on Legislation and National Security. Under his leadership, the Government Operations Committee has initiated oversight investigations and has issued reports that have saved billions of dollars and have greatly increased the efficiency of the federal government. Brooks has been a member of the House Judiciary Committee since 1955 and ranking Democrat since 1975, and he played a major role in writing the Civil Rights Act of 1964 and the Voting Rights Act of 1974.

This article is part of our special invited series by public officials designed to inform psychologists about policy issues of concern to psychology and the public at large. The views expressed are those of the author and do not necessarily reflect the views of the American Psychological Association or its officers.

Requests for reprints should be sent to Representative Jack Brooks, Government Operations Committee, 2157 Rayburn Building, Washington, D.C. 20515.

oversight committee in the House of Representatives and is empowered to review and investigate all government activities. Public hearings were held in which testimony was presented by knowledgeable witnesses. It was learned that, even excluding the National Security Agency (NSA) and the Central Intelligence Agency (CIA), federal agencies had conducted over 19,000 polygraph examinations in 1963. Although the scientific validity of polygraph testing had been at issue for years, there was virtually no scientific research to support its use. Federal witnesses testified, however, that their experience had shown the polygraph to be a helpful investigatory tool in national security cases. In its 1965 report, the committee concluded that "there is no 'lie detector,' neither machine nor human. People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood" (U.S. Congress, 1965, p. 1).

As a consequence, the committee favored a prohibition on the use of polygraphs in all but the most serious national security and criminal cases and then only when a guarantee could be provided that polygraph examinations would be voluntary. The committee also requested that an interagency committee be established to review and study the federal govenment's use of polygraphs.

The executive branch responded quickly to the committee's report. President Johnson established an interagency committee with representatives from DOD, the CIA, the Department of Justice (DOJ), and the Office of Science and Technology (OST) to study the polygraph. The DOD adopted its first polygraph directive (U.S. Department of Defense, 1965), which was reviewed by our committee. The committee was gratified by provisions of the regulation for stricter control of the conditions under which polygraph examinations would be given, more research, and the withdrawal of adverse consequences for refusal to take a polygraph test. The DOD regulations did, however, permit the standard use of polygraph examinations for preemployment screening—an area that hardly can be characterized as falling within the definition of the most serious national security cases (i.e., actual instances of security breaches). The committee recommended that personnel screening use should be immediately reconsidered. Further, it recommended that "qualified physicians and psychiatrists" should review polygraph examination records when they are given (U.S. Congress, 1966).

The committee's reactions to the results of the President's Interagency Polygraph Committee's work were similarly mixed. In line with our findings, the interagency committee concluded that there was insufficient scientific evidence concerning the validity and reliability of polygraph testing and that use of these instruments constituted an invasion of privacy of the individual under examination. The interagency committee recommended, as had the Government Operations Committee, that the "use of polygraphs in the Executive Branch should be generally prohibited and used only in special national security cases and in specified criminal cases" (personal communication to President Lyndon B. Johnson from the U.S. Civil Service Commission, July 29, 1966, p. 2). Apparently, the interagency committee had been convinced by testimony of the polygraph's usefulness in a number of espionage cases.

These recommendations, however, were never fully implemented. In 1973, the Civil Service Commission (now the Office of Personnel Management) issued specific government-wide regulations on the use of polygraphs for preemployment screening of competitive service applicants and appointees (U.S. Office of Personnel Management, 1973). The regulation prohibits the use of polygraph tests in screening for competitive service positions except for agencies that have a highly sensitive intelligence or counterintelligence mission directly affecting national security (e.g., a mission approaching the sensitivity of the Central Intelligence Agency). Such agencies are to be so certified by the chair of the Civil Service Committee on an annual basis. In addition, the regulation specifies that the refusal to consent to such an examination is not to be made a part of that person's personnel file. These rules are still in effect.

Unfortunately, the regulation is far too narrow to be considered as carrying out the recommendations of President Johnson's Interagency Polygraph Committee. It is relevant only to the use of polygraphs in personnel security screening interviews of competitive service applicants and appointees. The fact that it does not prohibit the use of polygraph tests in screening for exempted civil service employees means that the regulation only covers a portion of the federal work force. Excluded from the "competitive service" category are federal workers such as attorneys, cooks, chaplains, political appointees in the federal government, and employees not covered by the civil service regulation such as those employed in the Tennessee Valley Authority, the Federal Reserve System, and the Post Office. It was estimated that, in 1976, 250,000 to 375,000 civilian employees were not covered (U.S. Congress, 1976). Furthermore, the restrictions on including a refusal to take a polygraph examination in a person's file assume, of course, that an individual is hired. It does not restrict, in any manner, other uses of the polygraph tests. This authorization for the preemployment screening use of polygraph tests stands in contrast to the recommendation of the Government Operations Committee that polygraph use be restricted to "the most serious national security and criminal cases." As became clear, the investigation of specific incident situations calls for significantly different polygraph testing techniques than does personnel screening (cf. U.S. Congress, 1983b).

Despite the lukewarm nature of the federal policy response to our Committee's recommendations, polygraph use dropped substantially in the decade following the 1963 hearings. Over a decade after its first hearings, the Government Operations Committee, under my direction as chair, again reviewed the polygraph issue. In hearings before the Government Information and Individual Rights Subcommittee, we learned that the government's use of polygraphs had declined substantially since 1963. In fiscal year 1973, only 3,081 exams (over half done by the National Security Agency) were conducted, compared to the 19,796 figure for 1963, which excluded the CIA's and NSA's numbers.

Further, the committee found that only one agency, the Department of Defense, had requested to be certified under the regulation to use polygraph exams in conjunction with screening for competitive service employment. This request had not been granted because it did not conform with the *Federal Personnel Manual's* (U.S. Office of Personnel Management, 1973) requirements. The manual was useful then as it precipitated further changes to DOD's regulations. However, on a larger scale, in the absence of an appropriate reporting requirement, the Committee could not determine if the *Federal Personnel Manual* was being followed and working.

The committee did discover that other agencies had regulations at odds with the *Federal Personnel Manual* or were conducting exams that might be in violation of it because no distinction was being made between competitive service and other employees.

Perhaps most important, the 1976 Committee found that there had not been much new research on polygraph validity since 1963. It concluded that

> the nature of research undertaken, both federally and privately funded, and the results therefrom, have done little to persuade the committee that polygraphs have demonstrated either their validity or reliability in differentiating between truth or deception, other than possibly in a laboratory situation. (U.S. Congress, 1976, p. 12)

The committee recommended a complete ban on the use of polygraphs by all federal government agencies for all purposes. As with others, this recommendation has not been heeded.

The Reagan Administration's Polygraph Initiative

The Washington Post (Wilson, 1982) ran a cover story that reported a secret session of DOD's Defense Resources Board. The story reported that high-level Pentagon officials were informed of internal estimates that President Reagan's defense buildup would far exceed the $1.5 trillion the White House was publicly claiming. Again, as with the TFX incident almost 20 years earlier, a leak that was embarrassing but not a serious national security problem prompted an investigation to find the source.

As part of an ensuing investigation over 30 Defense Department employees were polygraphed. Many were tested without any prior questioning, despite the Department's polygraph regulation that had originated back in the 1960s to prevent such use of the technique. In its policy statement, the existing DOD directive provided that "the polygraph shall be employed only as an aid to support other investigative techniques and be utilized generally only after the investigation by other means has been as thorough as circumstances permit" (U.S. Department of Defense, 1975, p. 2). Based on the polygraph testing by DOD in response to the *Washington Post* leak, a suspect was identified and was given notice of his removal. But the reporter who had written the story came forward to say that the individual was not his source. The removal was halted and, instead, a reprimand was issued for disregarding DOD regulations, although not for "leaking," and the investigation ended.

As Chair of the Government Operations Committee and its Legislation and National Security Subcommittee, I viewed this incident with alarm. I requested the General Accounting Office (GAO), an investigative arm of the Congress, to review the Defense Department's investigation. They indicated that this investigation set a precedent for DOD "leak" investigations, both in terms of the number and level of officials involved. Further, the GAO discovered that of the 68 DOD investigations of "leaks" since 1975, in only one instance had the polygraph been used and then with only one employee who was the only suspect.

However, despite the extensive use of polygraphs in the Defense Resources Board investigation, the GAO concluded that it had been technically conducted in compliance with the DOD's regulations. In GAO's view, the word "generally" in the policy gave DOD leeway to conduct the investigation in the way it had (personal communication from William S. Anderson, General Accounting Office, to Jack Brooks, October 7, 1983).

Apparently undaunted by the lack of success with the polygraph in the DOD investigation, President Reagan issued a National Security Decision Directive in March 1983 (U.S. Department of Justice, 1983). Press accounts attributed him with contending that he was "up to his kiester" with leaks. Among other elements, the directive required all agencies to implement regulations that would require employees to take polygraph examinations in the course of leak investigations. Refusal to submit to such tests could result in adverse consequences such as reassignment or withdrawal of access to classified information.

At the same time, the Department of Defense was proposing revisions to their polygraph regulations to greatly expand their use from specific incident investigation purposes to preemployment, preaccess, and continuing random security checks. Like the President, the Department of Defense was proposing the threat of "adverse consequences" for those who refused to take the examinations.

It became clear that a massive policy change was underway. The Administration was seeking both quantitative and qualitative changes in the use of the polygraph. These changes were being implemented without apparent need or assurance that the new policies were scientifically or politically sound. Congressional oversight was urgently needed to evaluate this radical departure from past practice. Because the issue was so urgent, in July 1982, I sought and obtained an amendment to the Defense Department authorization, legislation that prevented implementation of any changes in the DOD's polygraph regulations until April 15, 1984.

In addition, under my direction the Legislation and National Security Subcommittee began an extensive review of these new polygraph policies. As part of its review, the Subcommittee asked the GAO to determine the prior and proposed use of polygraphs throughout the entire federal government. However, from earlier experiences I knew that the fundamental issue in assessing the government's polygraph programs was a determination, to the extent possible, of the *validity* of polygraph testing. If the polygraph could not be shown to work for the purposes proposed, then it should not be used by the government. Other considerations, such as individual privacy, search and seizure (Craig, 1984), and self-incrimination would come to the fore as policy questions only if it was concluded that the test works.

A clear-cut determination of validity was needed. To assist the committee in this task, Representative Frank Horton, the ranking Republican on the committee, and I turned to the Office of Technology Assessment (OTA). OTA was asked to critically review all the available scientific literature relating to the validity of polygraph testing and advise Congress as to its validity.

OTA's conclusions (U.S. Congress, 1983b) about validity of the polygraph under the Administration's proposed uses were disturbing. One finding confirmed our emphasis on limiting polygraph testing to the investigation of specific cases. OTA found that the polygraph question technique used depended on the use to which the test was put and that the technique with the most extensive research base was not the technique used in preemployment and preaccess screening. For the proposed screening uses, OTA found only four relevant studies, two of which had been conducted by the DOD. Unfortunately, only two specifically addressed validity (one of these was a DOD study). According to OTA "all had serious limitations in study design" (pp. 1–4). Further, OTA found no studies specifically related to wide scale investigations, so-called dragnet investigations. The possibility of dragnet investigations was inherent in the President's Directive, and the DOD had demonstrated their willingness to use them in this manner.

In the context of narrow specific-incident investigations (generally criminal) OTA found extensive research on validity; however, studies varied widely in their conclusions. In 28 studies presenting "acceptable scientific criteria," correct guilty detections ranged from 35% to 100%. Correct innocent detections ranged from 12.5% to 94%. None of these studied national security investigations. Further, OTA found that, in any context, coercing persons to take a polygraph test could theoretically affect validity, although no research had been conducted on this point.

Both the GAO and the OTA, as well as other interested witnesses, presented their findings at the committee's public hearing in October 1983. The GAO's statistics confirmed that the Administration's proposals were sweeping in scope. Under the terms of the president's directive, almost half the federal work force, or over 2.5 million government employees and about 1.5 million contractor employees, were potentially exposed to polygraph exams in leak investigations. Under just one provision of the DOD changes, over 116,000 employees with special security clearances could be subjected to random polygraph security checks. Nevertheless, Richard Willard of the Department of Justice announced additional Administration plans to permit government-wide polygraph use in personnel security screening of employees (and applicants for positions) with access to highly classified information.

Thus, the controversy continues. In its most recent report (U.S. Congress, 1983a), the Government Operations Committee concluded that "the validity of the polygraph is not scientifically supported for the purposes and manner of its proposed use" (p. 13) and recommended against the implementation of the Administration's new polygraph scheme. Public statements by high executive officials discredited the Administration's polygraph policies. Michael Deaver, the President's Deputy Chief of Staff, indicated that he did not support the use of lie detectors to ferret out White House leakers. Secretary of State, George Schultz, concurred, stating to editors of the *Washington Post* ("News Leakers Deserve Jail, Schultz Says," 1984) that "I'm not persuaded that lie detector tests are the thing to do by a long shot" (p. A19) when questioned about their use in tracking down the source of leaks. Several officials, including some in the White House, indicated an unwillingness to submit to tests to settle discrepancies in the Carter briefing book case. The Justice Department explained their subsequent decision not to use polygraphs in the case by saying it was Administration policy to only use polygraph tests when an investigatory purpose is to be served or there is evidence of a crime, an explanation that is inconsistent with the President's Directive and the Defense Department's proposals. The field office head who discussed polygraph plans with the press was quickly reassigned to the Portland, Oregon office by the FBI director. Media attention continued. Cartoons, depicting the President enthralled with polygraph machines and obsessed with secrecy, have become commonplace in the newspapers.

It is clear that the time has come for Congress to set polygraph policy for the federal government. In January 1984, I introduced H.R. 4681, the Federal Polygraph Limitation and Anti-Censorship Act of 1984, a bill that would correct problems uncovered in years of Government Operations Committee review. The bill would prohibit the use of polygraphs for any screening purposes, and would permit their use only in conjunction with a specific investigation into alleged criminal conduct (including the unauthorized disclosure of classified information) and then only when taken under absolutely voluntary conditions. Such testing could be conducted only after a thorough investigation, only for the development of additional information that is essential to that investigation. Tests could be administered only to an individual reasonably believed to have that information. The bill applies to all agencies of the federal government except the CIA and NSA.

This legislation was extensively reviewed by several House committees in the last Congress. Unfortunately, it was not acted upon by the full House prior to adjournment. I have reintroduced the legislation as H.R. 39 in this Congress, where it will again be considered.

Postscript

In February 1984, President Reagan indicated that he was suspending, at least until the end of the 98th Congress, the polygraph provisions of his directive. This move appeared to be an election year tactic, rather than a serious acknowledgment of flaws in the proposed policy.

Further, this suspension does not directly affect the Defense Department's polygraph plans. Congress has therefore provided for a freeze in the defense authorization bill on any changes to the department's polygraph policies for fiscal year 1985, except for authority to conduct a polygraph screening test program not to exceed 3,500 exams. Accordingly, DOD has begun such a test program this year. Ultimately, DOD intends to institute a coerced polygraph screening program that will cover over 100,000 employees and require the hiring of 50 new polygraph operators to enable them to conduct 10,000 new screening exams annually. Other agencies are following suit. For instance, the Justice Department intends to widen its polygraph screening program, and the Federal Emergency Management Agency has drawn up a polygraph screening program to be implemented for the first time at that agency (GAO, 1984). Apparently, the Administration continues to believe in the polygraph's efficacy. However, that belief is now based primarily on its utility, that is, its ability to elicit information from examinees and its presumed deterrent effect, neither of which have been evaluated scientifically.

Recently, the highly respected scientific journal, *Nature*, reported another scientific study demonstrating the fallibility of polygraph testing (Kleinmuntz & Szucko, 1984). They indicated that "these data, with their unacceptably high error rates, agree with the conclusions reached in a recent U.S. Congress Office of Technology Assessment report" (pp. 449–450). Kleimuntz and Szucko's research is yet another clear indication of the problematic nature of polygraph test validity.

Given the history of bureaucratic initiative in this area, despite repeated recommendations to the contrary and mounting scientific evidence exposing the invalidity of polygraph testing, the Administration has not proposed a very satisfying solution to the current impasse. It is vague, noncomprehensive, and only temporary. Legislation controlling the use of polygraphs within the federal government must be enacted if we are to avoid the cyclical, but steady, proliferation of unwarranted and inaccurate polygraph testing in the government.

The proponents of greater polygraph use by the federal government cite national security concerns to justify their positions. They assume that the testing is accurate and dismiss the negative effects on individuals' rights and privacy as acceptable costs for an enhanced national defense. However, the assumption of accuracy is faulty; the validity of polygraph testing is not scientifically supported. National security concerns, alone, argue against the greater use of polygraph screening. Reliance on this unsupported technique may create a false sense of security, thereby endangering not enhancing our security interests.

REFERENCES

Craig, J. (1984). The presidental polygraph order and the fourth amendment: Subjecting federal employees to warrantless searches. *Cornell Law Review, 69,* 896–924.

Fryklund, R. (1963, March 21). Air Force charges TFX "abuse." *Evening Star,* p. 1.

General Accounting Office. (1984). Polygraph and pre-publication review policies of Federal agencies (GAO/NSIAD-84-134). Washington, DC: U.S. Government Printing Office.

H.R. 4681, 98th Cong., 2nd Sess. (1984).

Kleinmuntz, B., & Szucko, J. J. (1984). A field study of the fallibility of polygraphic lie detection. *Nature, 308,* 449–450.

Lie detectors in the Pentagon. (1963, April 6). *New York Times,* p. 18.

News leakers deserve jail, Schultz says. (1984, April 6). *Washington Post,* p. A19.

Public papers of the Presidents of the United States January 1 to November 22, 1963. (1963). Washington, DC: U.S. Government Printing Office.

U.S. Congress, House Committee on Government Operations, Subcommittee on Government Information and Foreign Operations. (1965). *Use of polygraphs as "lie detectors" by the federal government* (House Report No. 198). Washington, DC: U.S. Government Printing Office.

U.S. Congress, House Committee on Government Operations, Subcommittee on Government Information and Foreign Operations. (1966). *Use of polygraphs as lie detectors by the federal government* (Part 2; House Report No. 280V). Washington, DC: U.S. Government Printing Office.

U.S. Congress, House Committee on Government Operations. (1976). *The use of polygraphs and similar devices by federal agencies* [Thirteenth report by the Committee on Government Operations together with separate and dissenting views]. Washington, DC: U.S. Government Printing Office.

U.S. Congress, House Committee on Government Operations. (1983a). *The Administration's initiatives to expand polygraph use and impose lifelong censorship on thousands of government employees* (House Report No. 98-578). Washington, DC: U.S. Government Printing Office.

U. S. Congress, Office of Technology Assessment. (1983b, November). *Scientific validity of polygraph testing: A research review and evaluation* (OTA-TM-H-15). Washington, DC: Office of Technology Assessment.

U.S. Department of Defense. (1965, July 13). *Conduct of polygraph examinations and the selection, training and supervision of DOD polygraph examiners* (Department of Defense Directive, No. 5210.48). Washington, DC: Author.

U.S. Department of Defense. (1975, October 6). *Polygraph examinations and examiners* (Department of Defense Directive, No. 5210.48). Washington, DC: Author.

U.S. Department of Justice. (1983). *Presidential directive on safeguarding national security information.* Washington, DC: Author.

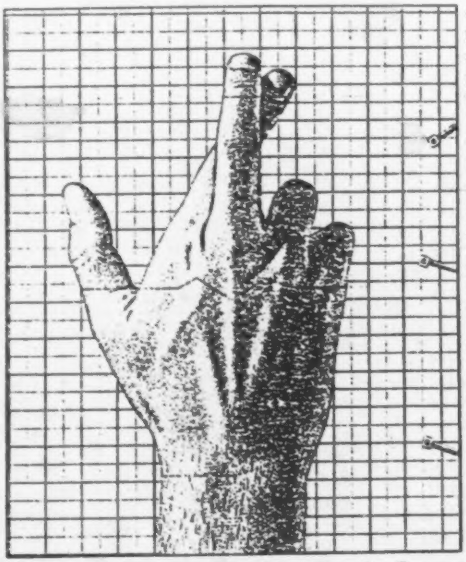
U.S. Office of Personnel Management. (1973). Use of the polygraph in personnel investigations of competitive service applicants and appointees to competitive service positions. *Federal personnel manual system* (ch. 736, app. D). Washington, DC: Author.

Wilson, G. (1982, January 8). Arms cost could exceed plan by $750 billion, leaders told. *Washington Post,* p. 1.

The Atlantic Monthly
oct 1984

SOME TRUTHS ABOUT LIE DETECTORS

Just how scientifically valid are polygraph tests? by Stephen Budiansky



Even allowing for the fact that Americans love gadgets, it is hard to explain the popularity of the lie detector. The roots of this invention, more formally known as the polygraph, go back to the turn of the century, when infatuation with the newly discovered powers of electricity more than once overcame common sense. But whereas electric hair-restorers and high-voltage cancer cures have all but vanished, the polygraph persists, and even flourishes. According to the best estimates, 1 million polygraph examinations are administered each year in the United States; they are used in criminal investigations, during government security checks, and, increasingly, by nervous employers—particularly banks and stores.

Those of us who are not among the 1 million examined each year have a number of opportunities to experience the polygraph vicariously. Celebrities accused of wrongdoing (John DeLorean comes to mind) invariably seem to offer to submit to polygraph examinations. Then there was the television program "Lie Detector," a 1983 show in which F. Lee Bailey, the polygraphist turned lawyer, added the dimension of home entertainment to polygraph tests.

Organized opposition to the increasing use of the polygraph has scored a modest success with the argument that the machine represents an invasion of privacy, especially when the coercive power of the government or an employer is behind it. It is very hard for a job applicant to say no when a prospective employer asks him or her to take a polygraph test; once hooked up to the machine, the applicant typically faces questions not only about past criminal activity but also about matters that an employer may have no business intruding upon, such as sexual practices or gambling—questions asked ostensibly in order to assess the applicant's "character." Retailers sometimes use the polygraph on current employees to ask questions like "Are you relatively satisfied with this job now?" and "Do you intend to stay with this employer?" As a result of such abuses, 19 states and the District of Columbia have made it illegal for an organization to ask its employees to subject themselves to polygraph examinations.

Much the same issue is at the heart of the protracted wrangle between the Reagan administration and Congress over plans for expanded government use of the polygraph. An executive order issued on March 11, 1983, known as National Security Decision Directive 84, would have sanctioned for the first time "adverse consequences" for a federal employee who refuses to take a test when asked. The directive authorized tests to investigate candidates for certain security clearances and to ask any federal employee about leaks of classified information. (It was issued shortly after

ILLUSTRATION: BEN LUCE

Reagan's comment about being "up to my keister" in press leaks.) Almost simultaneously the Department of Defense (DOD) released a draft regulation that authorized use of the polygraph to screen employees who take on certain sensitive intelligence assignments; it, too, prescribed adverse consequences for refusal.

Both proposals are now in abeyance. Although a congressional ban on changes in DOD polygraph policies expired on April 15 of this year, the DOD and Robert McFarlane, the national security adviser, sent assurances to Capitol Hill that they would not proceed with any proposed changes "during the remainder of this session of Congress." Both left little doubt, however, that the proposals are very much alive. Congressman Jack Brooks, a Democrat from Texas, has introduced a bill that would kill the proposals once and for all, restrict use of the polygraph to criminal investigations, and require consent from the examinee. In a bow to political reality the bill exempts the Central Intelligence Agency and the National Security Agency.

A question more basic than whether the polygraph test is an unacceptable invasion of privacy is, of course, whether it works. Seeking an answer in the scientific literature can be a bewildering experience. A report by the Office of Technology Assessment (OTA), commissioned last year by Brooks's Committee on Government Operations, summed up the problem by citing 24 studies that found correct-detection-of-guilt rates ranging from 35 to 100 percent.

The flourishing polygraph industry (it is estimated that there are at least five thousand professional polygraphists in the country) naturally looks on the bright side of these studies. Sergeant Kenneth Shiflet of the Colorado State Patrol, a past president of the American Association of Police Polygraphists, says that polygraph results are "at least ninety-five percent accu-

Teach your word processor to read.

Whether you have a CPT, Exxon, IBM, Lanier, NBI, Wang or Xerox, we can make it smarter. The compact Dest WorkLess Station™ lets you enter typewritten pages of different typestyles into your word processor automatically, without using the keyboard.

For immediate information and the name of your nearest dealer, call Mary Thorpe at (800) 538-7582. In California, call (408) 946-7100. Or fill out and mail this coupon to Dest Corporation, 1201 Cadillac Ct., Milpitas, CA 95035.

The WorkLess Station. The Dest way to improve word processing. DEST

My word processor is a ________

NAME ________

COMPANY ________

ADDRESS ________ CITY ________

STATE ________ ZIP ________ PHONE ________

12-EA

DEST and WorkLess Station are trademarks of Dest Corporation

Gables Laroc
Coral Gables, Florida, USA

32 of the most luxurious condominium homes in South Florida's most prestigious community. Located in the heart of Coral Gables, heralded as the international city of today, Gables Laroc is within minutes of international restaurants, theaters, fabulous shopping, international banking and superb athletic and country club facilities. And only ten minutes away from Miami International Airport. Though close to everything, Gables Laroc is set back on a quiet, secluded, elegant street.

LAROC

441 Valencia Avenue, Coral Gables, FL 33134, Telephone: (305) 444-1091

SWEEPING 3-BEDROOM, 2-1/2 BATH, CHEERY 3-BEDROOM, 2-1/2 BATH, LIGHT AND AIRY 2-BEDROOM, 2 BATH — AND A BREATHTAKING PENTHOUSE FLOOR, WITH EVERY AMENITY NEEDED FOR A LEISURELY LIFE, INCLUDING YEAR-ROUND TROPICAL SUN. PRICES RANGE FROM $170,000 TO OVER $500,000.

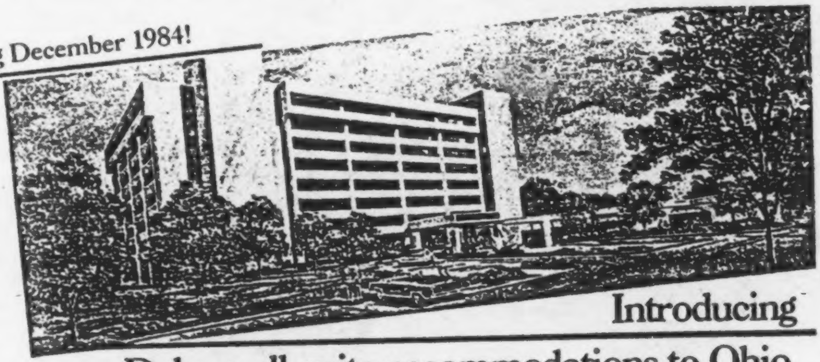
rate." Joseph Buckley, the president of John E. Reid and Associates, one of the oldest polygraph firms in America, puts accuracy at 85 to 95 percent.

Skepticism comes mostly from psychologists, whose studies report substantially lower accuracy rates, generally around 70 percent. Picking one's way through the scientific debate is not made any easier by the obvious social and intellectual friction between the two camps. "You have to bear in mind that you have academics coming into this field," Buckley says. "Many of them are nontrained, nonexaminer people." David Lykken, a professor of psychiatry at the University of Minnesota and a major critic of the validity of polygraph testing, counters that the average training program for a professional polygraph examiner lasts six to eight weeks—"about one-sixth the study time required by the average barber college."

To evaluate the rival claims, a person needs little more than common sense and a basic knowledge of statistics. The first step is to find out where the numbers that support the accuracy of the polygraph come from. Significantly, the most optimistic of the optimists is Norman Ansley, the chief of the polygraph division of the National Security Agency's Office of Security. The NSA leads the roster of federal polygraph users; both it and the CIA rely heavily on polygraph testing for preemployment and routine security screening. The NSA reported giving nearly ten thousand tests in 1982. (CIA numbers are classified.)

A review article written by Ansley last year reported an average of 97.6 percent accuracy in studies in which a polygraphist's diagnosis of "truthful" or "deceptive" was compared with some independent measure of the subject's guilt or innocence, such as a subsequent confession or an evaluation of guilt by an expert judicial panel that had reviewed other material evidence in the case. The polygraphists' diagnoses were correct at least 90 percent of the time in all of these instances.

Yet the research Ansley chose to include in his review is problematic. Even the OTA report, which at times seemed to bend over backward to accommodate all points of view, disqualified from its consideration all but one of the eight field studies that Ansley cited, finding statistical problems with some and dismissing others as "anecdotal." ▶



Opening December 1984!

Introducing

Deluxe all-suite accommodations to Ohio.

LOCATION:
In Columbus, at I-270 and Cleveland Avenue in the Corporate Exchange Office Complex. Just a 20-minute drive from downtown. 15-minutes from Ohio State University and Columbus International Airport. Only 1 mile from Busch Corporate Center.

ATTRACTIONS:
222 luxurious 2-room suites. Complimentary full breakfast. Cocktail party included in room rate, daily 5-7 p.m. 4100 sq. ft. ballroom. Plus executive conference suites and board room. Restaurant and lounge with live entertainment.

SUITES:
Many feature bedroom with king size bed. Luxurious bath. Separate living room with conference and dining area. Kitchen area with refrigerator, microwave oven and wet bar.

RATES:
Priced with or below major chain hotels.
-Weekdays: Monday thru Thursday. Single from $79; Double from $89.
Weekends: Friday, Saturday or Sunday. Single from $59; Double from $69.

RECREATION:
Indoor/Outdoor heated pool. Measured jogging track. Exercise room with equipment. Whirlpool.

GRANADA ROYALE

EMBASSY SUITES HOTEL

Operated by The Continental Companies

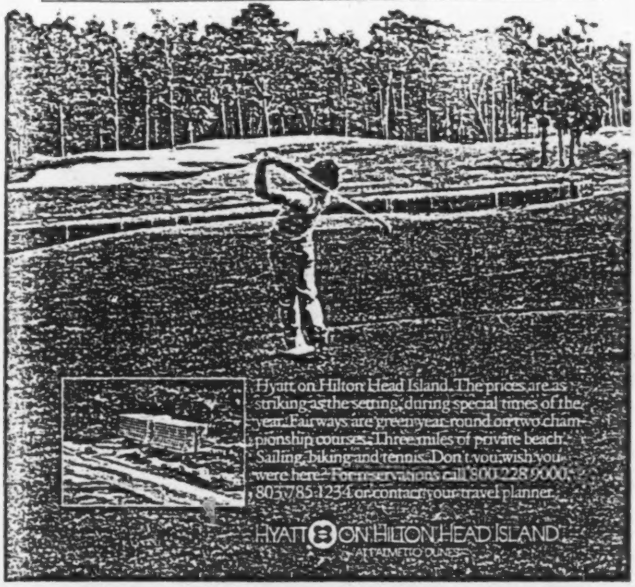
2700 Corporate Exchange Drive • Columbus, Ohio 43229
1-800-EMBASSY

The OTA report did not elaborate. But one of these "anecdotal" studies was in fact nothing more than a survey of polygraphists, who were asked how many tests they had administered, how many had been verified, and how many of those they got right. Lykken observed in congressional testimony last year that a similar questionnaire sent to astrologers would produce similar results.

The proliferation of statistical measures of accuracy is itself a source of overstatement of polygraphic accuracy. Proponents of the polygraph will, for example, sometimes cite "correct guilty detections": the percentage of guilty subjects who are caught by the polygraph. This figure can be very impressive; in one study that does not suffer from the failings already mentioned, it was 98 percent. But the same study found that 55 percent of *innocent* subjects were also diagnosed as "deceptive." The handful of studies that used a truly random selection of cases and rescored them blind produced similar results: overall, 83 percent of guilty subjects were diagnosed as "deceptive," as were 43 percent of innocent subjects. It's no trick to push the correct-guilty-detection rate up to 100 percent—just call everyone "deceptive." You don't even need a machine to do that.

Given all the doubts about validity, why does the government persist in using polygraph tests? Some clues are found in the Defense Department's 1983 report on polygraph testing—and even in its title, "The Accuracy and Utility of Polygraph Testing," which suggests that accuracy and utility are two different things. The most that the report concludes about accuracy is that it is "significantly above chance." Utility, however, is quite another matter: "Where examinees are found deceptive during testing, the confession rate is consistently high." The report gives example after example of examinees who confessed to criminal or espionage

STRIKINGLY HILTON HEAD.



Hyatt on Hilton Head Island. The prices are as striking as the setting, during special times of the year. Fairways are green year round on two championship courses. Three miles of private beach. Sailing, biking and tennis. Don't you wish you were here? For reservations call 800 228 9000, 803 785 1234 or contact your travel planner.

HYATT ON HILTON HEAD ISLAND
AT PALMETTO DUNES

OMNIFAX®

Affordable Transportable Fax!

Less than $3,000 for briefcase-size fax with features many larger machines don't have. Fully automatic operation. Sends and receives fine resolution copy, drawings and more—to and from virtually any fax. Groups 3, 2, 1, 9600 BPS. Even leaves callback message. Ideal for office or travel needs. Sold and serviced by Telautograph Corporation in the U.S., Canada and Puerto Rico. For brochure or demonstration CALL TOLL FREE, ask for Operator 553.

800-824-7888

Alaska & Hawaii
800-824-7919

*Omnifax is a registered trademark of Telautograph Corp.

activity. The star is an NSA job applicant who "admitted that his engineering degree was phony (he bought it through mail order from London for $100)," that he "shot and wounded his second wife," and that his present wife "is missing under unusual circumstances that he would not explain."

One DOD official who lodged an internal protest against the department's new polygraph policy received a similar explanation of the polygraph's utility from General Richard Stilwell, the undersecretary of defense and the architect of the policy. In response to a memo setting out scientific objections to the polygraph in some detail, Dr. John Beary, the acting assistant secretary of defense for health affairs, received an icy note from Stilwell that skipped over the scientific issues (except to mention Ansley's review article and how "well received" Ansley had been at congressional hearings) and pointedly asked Beary how he viewed "the utility of the polygraph process in light of its demonstrated value at CIA and NSA."

Among all defense officials who were asked to comment on the new policy, only Beary refused to give it his approval. Soon afterward he left the Defense Department, and late last year Stilwell reported to Secretary of Defense Caspar Weinberger that "following Dr. Beary's departure, a concurrence has been obtained from OASD (Health Affairs)."

Not long before Beary left, obviously frustrated at getting nowhere with his scientific arguments, he sent another memo to Stilwell. "One could reasonably ask," he wrote, "why has Washington been bamboozled by the polygraph community for more than twenty years? I can only speculate that it may have something to do with the poor state of science education in the United States." ☐

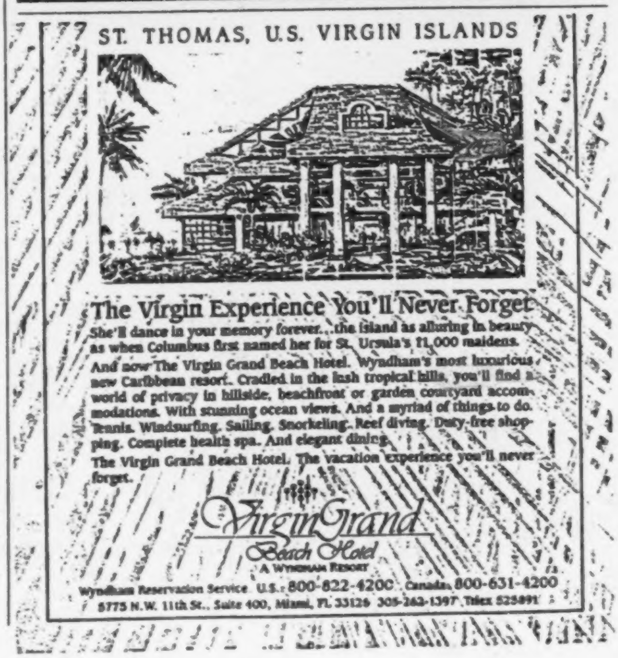
Copyright © 1984 by Stephen Budiansky.

No Other Resort Even Comes Close

Neither Does Civilization. Indian River Plantation on Hutchinson Island, one of the [illegible] Florida's east coast. Explore [illegible] sandy beach. Inhale [illegible] gorgeous par 61 course [illegible] 13 tennis courts [illegible]

INDIAN RIVER PLANTATION RESORT
Hutchinson Island
385 N.E. Plantation Road
Stuart, Florida 33494

For more information, call toll free:
1-800-327-4873
Above the Palm Beaches on beautiful Hutchinson Island.


ST. THOMAS, U.S. VIRGIN ISLANDS

The Virgin Experience You'll Never Forget

She'll dance in your memory forever... the island as alluring in beauty as when Columbus first named her for St. Ursula's 11,000 maidens.

And now The Virgin Grand Beach Hotel. Wyndham's most luxurious new Caribbean resort. Cradled in the lush tropical hills, you'll find a world of privacy in hillside, beachfront or garden courtyard accommodations. With stunning ocean views. And a myriad of things to do. Tennis. Windsurfing. Sailing. Snorkeling. Reef diving. Duty-free shopping. Complete health spa. And elegant dining.

The Virgin Grand Beach Hotel. The vacation experience you'll never forget.

Virgin Grand Beach Hotel
A Wyndham Resort

Wyndham Reservation Service U.S.: 800-822-4200 Canada: 800-631-4200
5775 N.W. 11th St., Suite 400, Miami, FL 33126 305-262-1397 Telex 525891

I

99TH CONGRESS
1ST SESSION

H. R. 39

Relating to the administration of polygraph examinations and prepublication review requirements by Federal agencies.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 3, 1985

Mr. BROOKS introduced the following bill; which was referred to the Committee on Post Office and Civil Service

---

A BILL

Relating to the administration of polygraph examinations and prepublication review requirements by Federal agencies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Polygraph Limitation and Anti-Censorship Act of 1984".

SEC. 2. (a) Chapter 73 of title 5, United States Code, is amended by adding at the end thereof the following new subchapter:

"SUBCHAPTER VI—POLYGRAPH EXAMINATION AND PREPUBLICATION REVIEW RESTRICTIONS

"§ 7361. Definitions

"For purposes of this subchapter—

"(1) the term 'agency' means—

"(A) an Executive agency;

"(B) the United States Postal Service;

"(C) the Postal Rate Commission;

"(D) the Administrative Office of the United States Courts;

"(E) the Library of Congress;

"(F) the Government Printing Office;

"(G) the Office of Technology Assessment;

"(H) the Congressional Budget Office;

"(I) the Office of the Architect of the Capitol; and

"(J) the Botanic Garden;

"(2) the term 'employee' means—

"(A) an individual employed by an agency;

"(B) a Congressional employee (other than an individual under subparagraph (A)); and

"(C) an expert or consultant who is under contract under section 3109 of this title with an agency, including, in the case of an organization performing services under such section, an individual involved in the performance of such services;

"(3) the term 'classified information' means information—

"(A) specifically authorized under criteria established by statute or Executive order to be kept secret in the interest of national defense or foreign policy; and

"(B) in fact properly classified pursuant to such statute or Executive order;

"(4) the term 'polygraph examination' means an interview with an individual which involves the use of a device designed to permit the examiner to make an inference or a determination, by evaluation of measured physiological responses, concerning whether the individual has truthfully or deceptively responded to inquiries made in such interview;

"(5) the term 'action', as used with respect to an employee or applicant for employment, means—

"(A) a personnel action under clauses (i) through (x) of section 2302(a)(2)(A) of this title;

"(B) a decision concerning clearance for access to classified information; and

"(C) a performance evaluation (other than under chapter 43 of this title);

in the case of such employee or applicant; and

"(6) the term 'prepublication review' means submission of information to an agency for the purpose of permitting such agency to examine, alter, excise, or otherwise edit or censor such information before it is publicly disclosed, but does not include any such submission with respect to information which is to be disclosed by an employee in such employee's official capacity.

"§ 7362. Restrictions relating to polygraph examinations

"(a) An agency may not—

"(1) require, threaten to require, or, except as provided in subsection (b), request any employee or applicant for employment to submit to a polygraph examination;

"(2) take, or threaten to take, any action against an employee or applicant for employment—

"(A) on the basis of that individual's refusal to submit to a polygraph examination; or

"(B) on the basis of any inference or determination (referred to in section 7361(4) of this title) made from that individual's performance in the course of a polygraph examination; or

"(3) fail to take, or threaten to fail to take, any action on behalf of an employee or applicant for employment—

"(A) on the basis of that individual's refusal to submit to a polygraph examination; or

"(B) on the basis of any inference or determination described in paragraph (2)(B).

"(b) An agency may request an employee, in writing, to submit voluntarily to a polygraph examination—

"(A) if the examination is administered as part of a specific investigation into alleged criminal conduct—

"(i) after the completion, by other means, of as thorough an investigation as circumstances reasonably permit; and

"(ii) solely for the development of information essential to that investigation;

"(B) if the individual is reasonably believed to have knowledge of the matter under investigation; and

"(C) if the alleged criminal conduct constitutes an offense punishable by death or imprisonment for a term exceeding one year.

"§ 7363. Restrictions relating to prepublication review

"An agency may not—

"(1) request, require, or threaten to require, an employee or applicant for employment to enter into an agreement, any part of which requires prepublication review;

"(2) take, or threaten to take, any action against an employee or applicant for employment on the basis of that individual's refusal to enter into such an agreement;

"(3) take, or threaten to take, any action against an employee or applicant for employment on the basis of that individual's refusal to comply with any of the provisions of such an agreement which require prepublication review;

"(4) fail to take, or threaten to fail to take, any action on behalf of an employee or applicant for employment on the basis of a refusal referred to in paragraph (2) or (3); or

"(5) establish or enforce, or threaten to establish or enforce, any other requirement in order to compel prepublication review.

"§ 7364. Remedies

"(a)(1) Subject to paragraph (2) and subsection (b), any person aggrieved by a violation of section 7362 or 7363 of this title may bring a civil action against the United States for equitable or monetary relief, or both, in the district court of the United States for the district in which that person resides, for the District of Columbia, or, in the case of an employee or former employee, for the district in which that person was employed at the time the cause of action arose.

"(2) A civil action under this subsection shall be forever barred unless commenced within two years after the cause of action arose. For purposes of this paragraph, a cause of action shall be deemed to have arisen on the date that the person aggrieved knew, or with reasonable diligence should have known, of the violation concerned.

"(3) The court shall award reasonable costs of litigation, and may award reasonable attorney fees, to a prevailing plaintiff in an action brought under this subsection.

"(b)(1) If a person aggrieved by a violation of section 7362 or 7363 of this title would also be entitled to initiate proceedings for remedial action under agency administrative procedures, such person may raise the matter under subsection (a) or under such administrative procedures, but not both.

"(2) A person shall be deemed to have exercised the option under this subsection to raise a matter either under subsection (a) or under agency administrative procedures upon the timely commencement of an action by such person in accordance with the Federal Rules of Civil Procedure or the timely initiation of such administrative procedures by such person, as the case may be.

"(3) For purposes of this subsection, the term 'agency administrative procedures' means any formal process of review by an agency provided under statute, regulation, or Executive order, including judicial review of any determination made in the course of such process.

"§ 7365. Exemptions

"Sections 7362 and 7363 of this title do not apply—

"(1) to the Central Intelligence Agency, in the case of any individual employed by, or detailed to, the Central Intelligence Agency, any individual applying for a position in the Central Intelligence Agency, or any expert or consultant under contract with the Central Intelligence Agency; or

"(2) to the National Security Agency, in the case of any individual employed by, or detailed to, the National Security Agency, any individual applying for a position in the National Security Agency, or any expert or consultant under contract with the National Security Agency.".

(b) The analysis for chapter 73 of title 5, United States Code, is amended by adding at the end thereof the following:

"SUBCHAPTER VI—POLYGRAPH EXAMINATION AND PREPUBLICATION REVIEW RESTRICTIONS

"7361. Definitions.
"7362. Restrictions relating to polygraph examinations.
"7363. Restrictions relating to prepublication review.
"7364. Remedies.
"7365. Exemptions.".

SEC. 3. (a)(1) The provisions of any agreement referred to in section 7363(1) of title 5, United States Code (as added by this Act) are, to the extent that such provisions relate to prepublication review, hereby rescinded.

(2) The head of each agency concerned shall provide written notice to each individual who, immediately before this Act takes effect, was a party to any such agreement, informing such individual of—

(A) the enactment of this section; and

(B) the provisions of the agreement rescinded as a result of the enactment of this section.

(b) Nothing in subsection (a) applies with respect to the Central Intelligence Agency or the National Security Agency, or to any agreement which requires prepublication review by either of those agencies.

(c) For purposes of this section, "prepublication review" and "agency" each has the meaning given that term in section 7361 of title 5, United States Code (as added by this Act).

SEC. 4. This Act shall take effect on April 15, 1984.

EXHIBIT NO. 19.--Communications side of security area. "Black vault" in background.

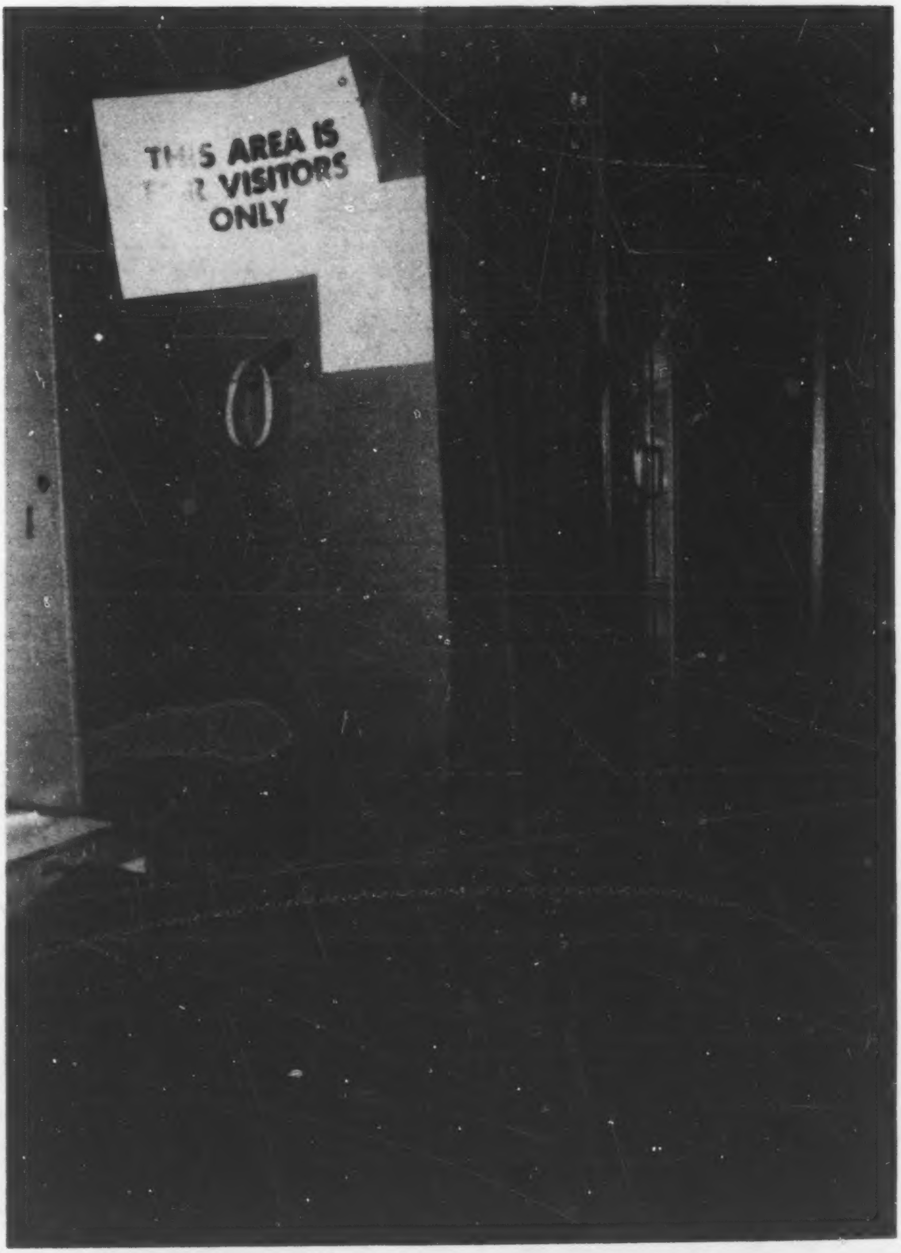

THIS AREA IS
FOR VISITORS
ONLY

EXHIBIT NO. 20.--Encrypting machine.

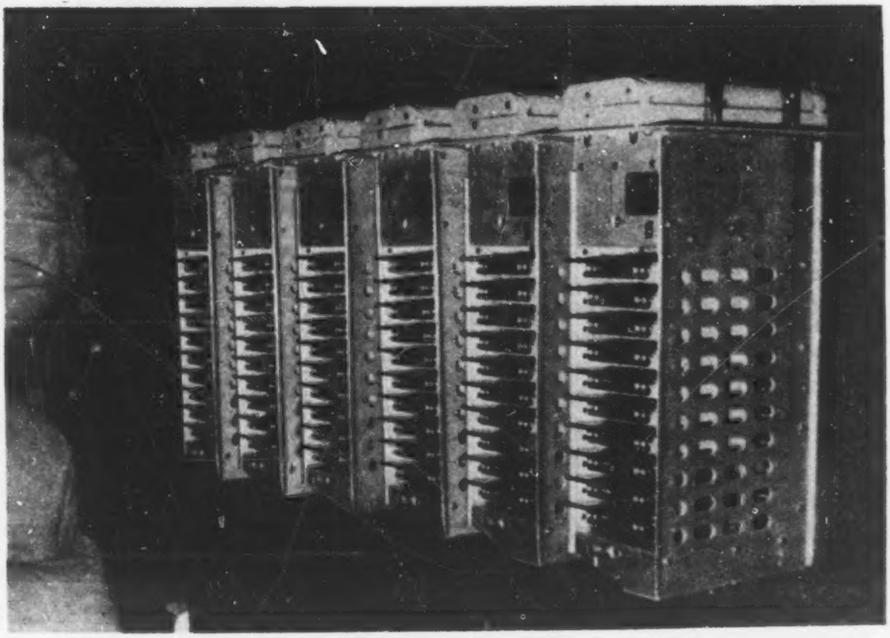


EXHIBIT NO. 21.--Encrypting device.

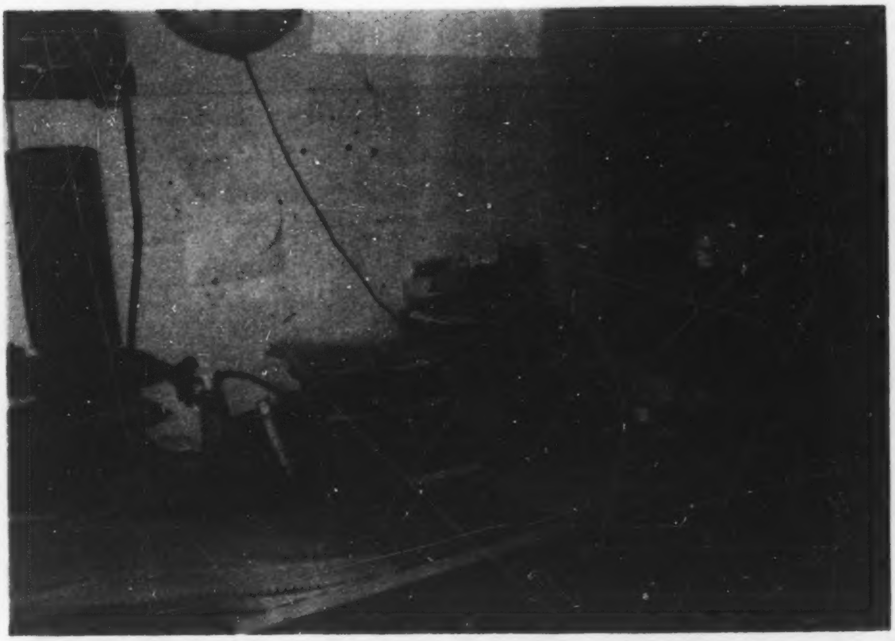


EXHIBIT NO. 22.--Log desk (where Minox used to photograph documents).

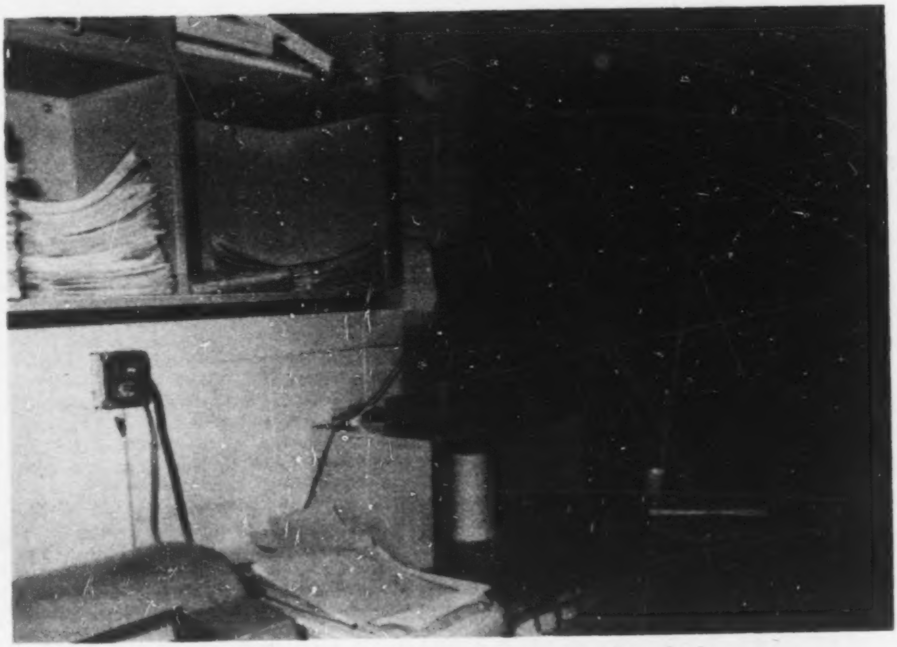


EXHIBIT NO. 23.--Outgoing TWX correction desk.

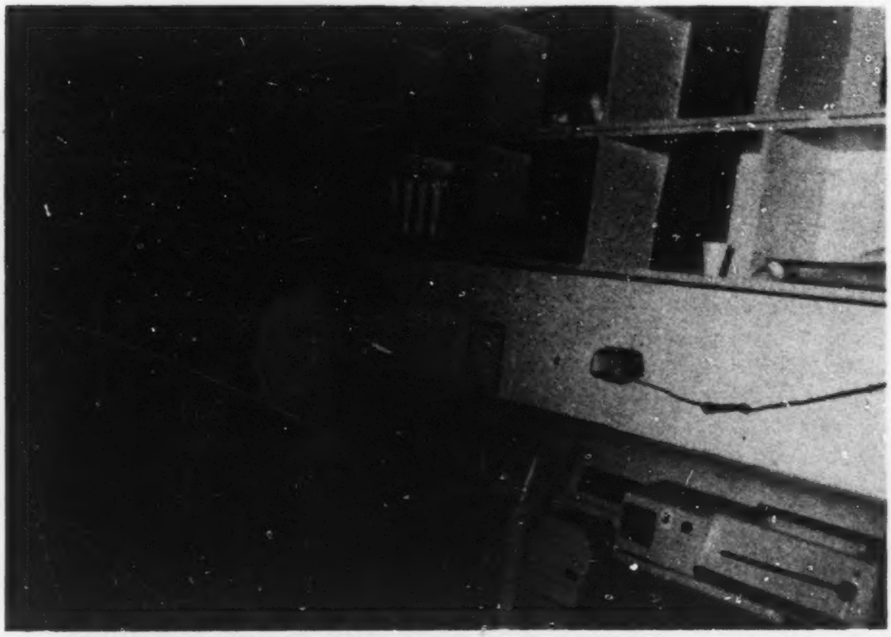


EXHIBIT NO. 24.--Inside of vault looking at Telex machines.

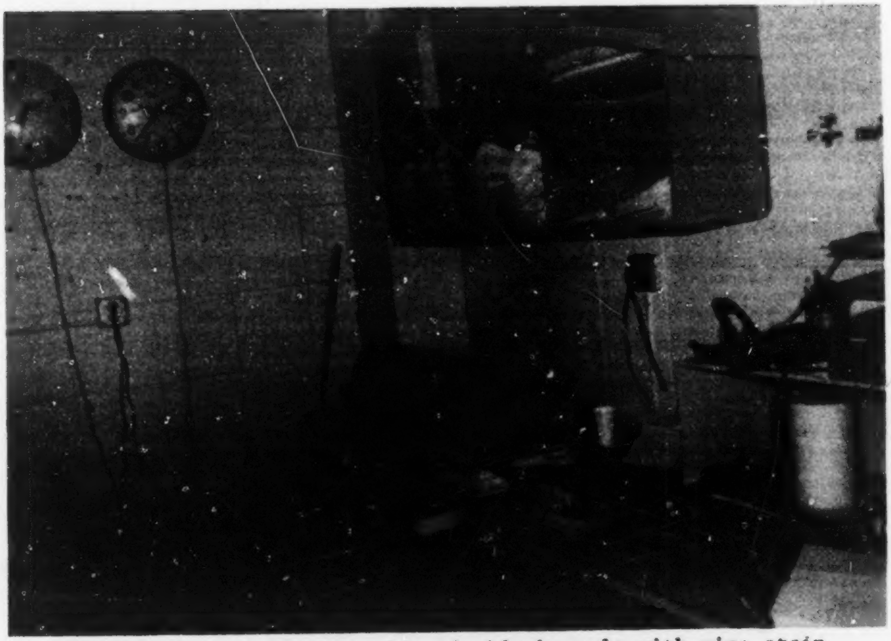


EXHIBIT NO. 25.--Telex machine in black vault with wine stain on wall.

○